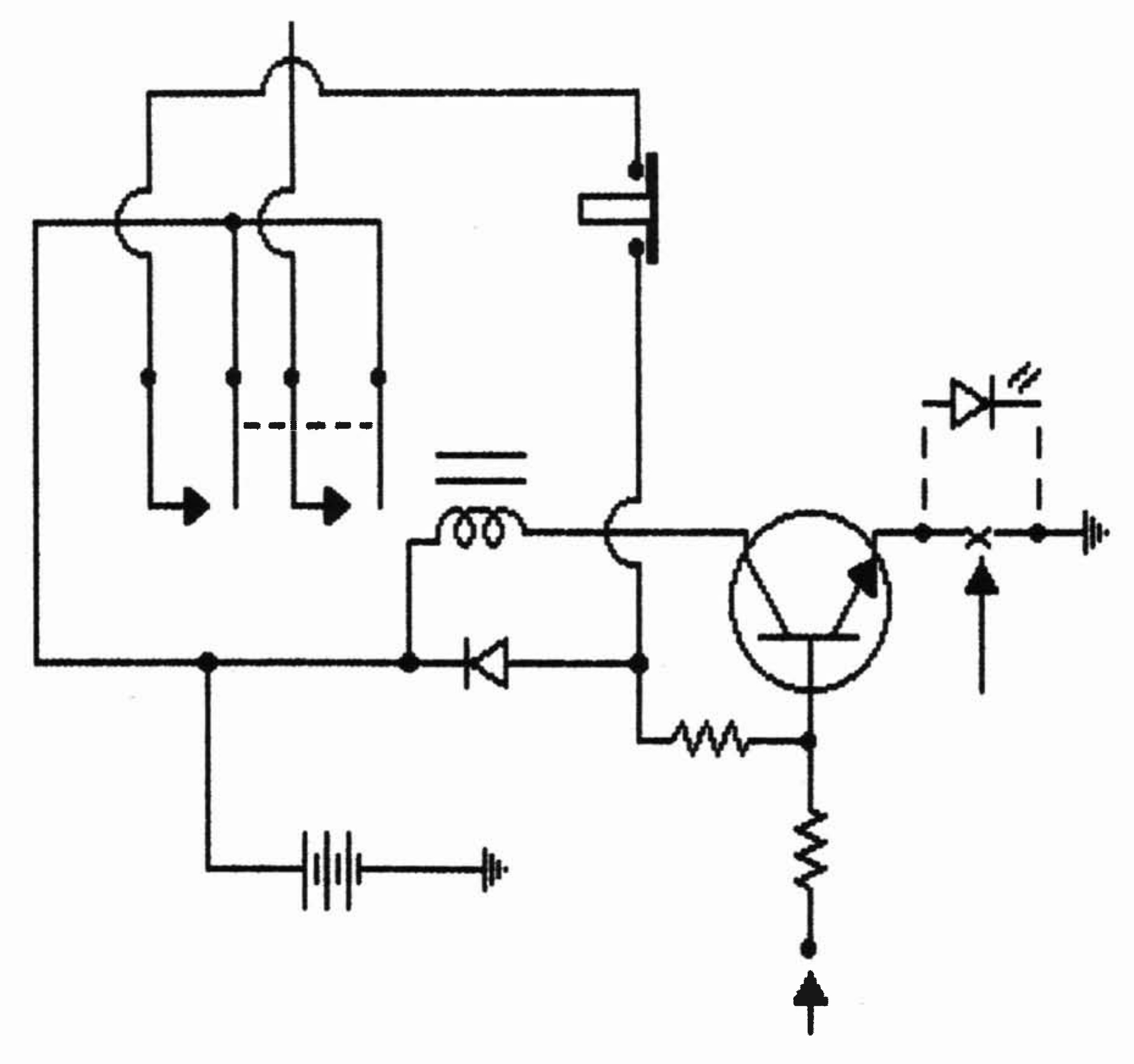
MORE BENCH-TESTED CIRCUITS

Innovative Designs for Surveillance and Countersurveillance Technicians



Tom Larsen

Paladin Press · Boulder, Colorado

Also by Tom Larsen:

Bench-Tested Circuits for Surveillance and Countersurveillance Technicians

The Layman's Guide to Electronic Eavesdropping

More Bench-Tested Circuits:
Innovative Designs for Surveillance
and Countersurveillance Technicians
by Tom Larsen

ISBN 1-58160-007-0
Printed in the United States of America

Published by Paladin Press, a division of
Paladin Enterprises, Inc., P.O. Box 1307,
Boulder, Colorado 80306, USA.
(303) 443-7250

Direct inquiries and/or orders to the above address.

CONTENTS

To A.N., for a "wire job" well done that
successfully nailed J.H. some 30 odd
years ago. Those electronic catalogs
(with their interesting offerings) that
you gave me when I was a young lad
were a real inspiration to me!
This book's for you!

PREFACE

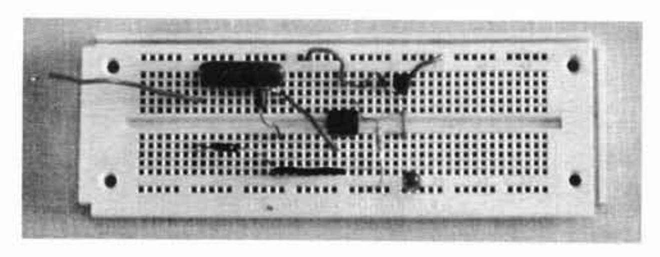
Just as in my first book in this series, *Bench-Tested Circuits for Surveillance and Countersurveillance Technicians* (Paladin Press, 1996), all of the circuits in this book were bench-tested, with the exception of the one discussed in "How to Modulate a Laser Beam" (p. 52).

This book was written for serious surveillance and countermeasures technicians, whether they are just breaking into the field or are "old pros." (Even an old dog can be taught new tricks.) In this book I concentrated a little more on stealthy phone tapping equipment and countermeasures alarm devices, that is, simple countermeasures that work while you sleep.

This book includes some never-published countermeasures techniques and phone-tapping methods. There are also some helpful diagnostic aids in Part III, the Miscellaneous section called "Bugger's Little Helpers." I also went a little lighter on the electronic math than I did in *Bench-Tested Circuits*. I did provide some theory on circuit operation where I felt it was needed.

The circuits presented in this book are my own creations and/or modifications of basic "generic building blocks." Please feel free to experiment and modify them to suit your personal needs. Many of the circuits in this book (as well as in the original *Bench-Tested Circuits*) were intended to be electronic "springboards" or "platforms" for new and improved devices. Please, take one of my circuits at a time and improve upon it for your personal requirements and enjoyment. I know some of you out there can do it!

I am assuming that you have, at the very least, a basic electronic knowledge, DVM, oscilloscope, and burning desire to learn and improve this industry! Hopefully we can "run the rain dancers out of Dodge on a rail." So many rain dancers, so little time . . .



Prototyping made very easy. The author used these very handy 6" modular bread boards for most of the circuits in this book. The circuit pictured is the ring detector portion (with an LED instead of a buzzer), which was used for the "Simple Telephone Isolation Circuit." These modular bread boards are readily available at most electronic suppliers, including Radio Shack.

WARNING

The author, publisher, and distributor assume no responsibility for misuse (legal or illegal) of the circuits, tips, and techniques presented in this book. When you are working around high voltage, caution and common sense should prevail! Many of the surveillance circuits, tips, and techniques in this book are illegal and are presented *for educational and demonstration purposes only.* Please consult the Electronic Communications Privacy Act of 1986 (ECPA) before you go into the business of spying on people.

SOME FIXES FOR THE ORIGINAL
Bench-Tested Circuits for Surveillance and Countersurveillance Technicians

1) Page 56: The NO switch to prevent false triggering on power-up should be NC (normally closed).

2) Page 83: The 200-ohm resistors are CO (they represent the central office resistors).

3) Page 98 (parts list): RCA phone jacks should be RCA *phono* jacks.

4) Page 101 (last paragraph): Same as above—RCA phone jacks should be RCA *phono* jacks.

5) Page 110: IC2 pin 12 should not be used; use pin 9. Pin 9 will give 8 counts.

6) Page 115: the CdS1 photoresistor does not emit light; the arrows should be pointing toward the CdS1.

NOTE FROM THE PUBLISHER: The above errors were present in early print runs only and have since been corrected. Current editions of *Bench-Tested Circuits* should reflect these corrections.

SECTION I

ELECTRONIC COUNTERMEASURES

(ELECTRONIC FLYSWATTERS)

POOR MAN'S COMPONENT SIGNATURE ANALYZER

In the late 1980s a private investigator friend of mine attended a seminar conducted by a former FBI agent. Following the seminar, my friend had a very interesting discussion during lunch with the former agent. The former FBI agent made the following claim: "Your countermeasures guy [that's me] would probably not be able to find the following bug that is commonly used by the FBI: it is a low-frequency, carrier-current, digital-modulation, and remote-shut-off transmitter."

Later that afternoon my PI friend called and told me what the former FBI agent said. By the next morning I had developed a simple device and technique that would readily expose this nefarious device as well as other devices connected to the power line.

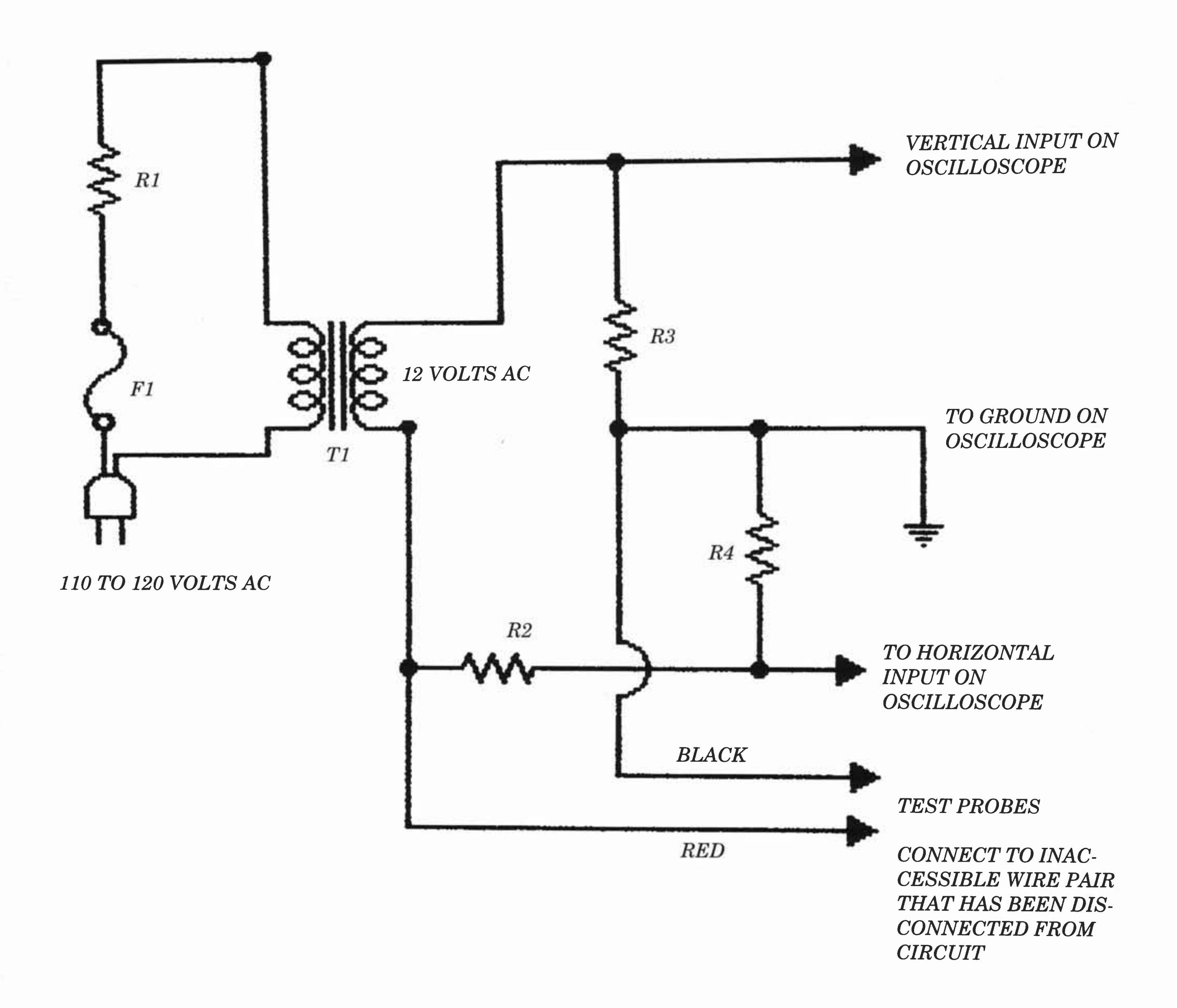
As one can imagine, there is a great deal of legwork involved in using the "Poor Man's Component Signature Analyzer." When analyzing an inaccessible power line that runs who knows where—through walls, ceilings, and basements—you must absolutely do the following: turn off the breaker for that circuit and make absolutely sure that all appliances are unplugged and that NOTHING is connected in parallel with the power line. Unscrew all light bulbs, as long as they are not connected to dimmer switches; this will permit you to analyze the circuit all the way to the lamp fixture.

I would strongly suggest that you test the AC power line with a neon circuit tester before you connect the "Poor Man's Component Signature Analyzer." You want to make sure that there is no power on the AC line! It would also be a good idea to do a signature analysis of various appliances, such as radios, TVs, washers, portable heaters, microwave ovens, doorbell transformers, and so on.

When you're in commercial buildings, you will have to disconnect ballasts to all fluorescent fixtures. It can get pretty involved!



Poor Man's Component Signature Analyzer. Assembly and packaging is very easy; however, don't let its simplicity fool you; this is a very powerful countermeasures tool!



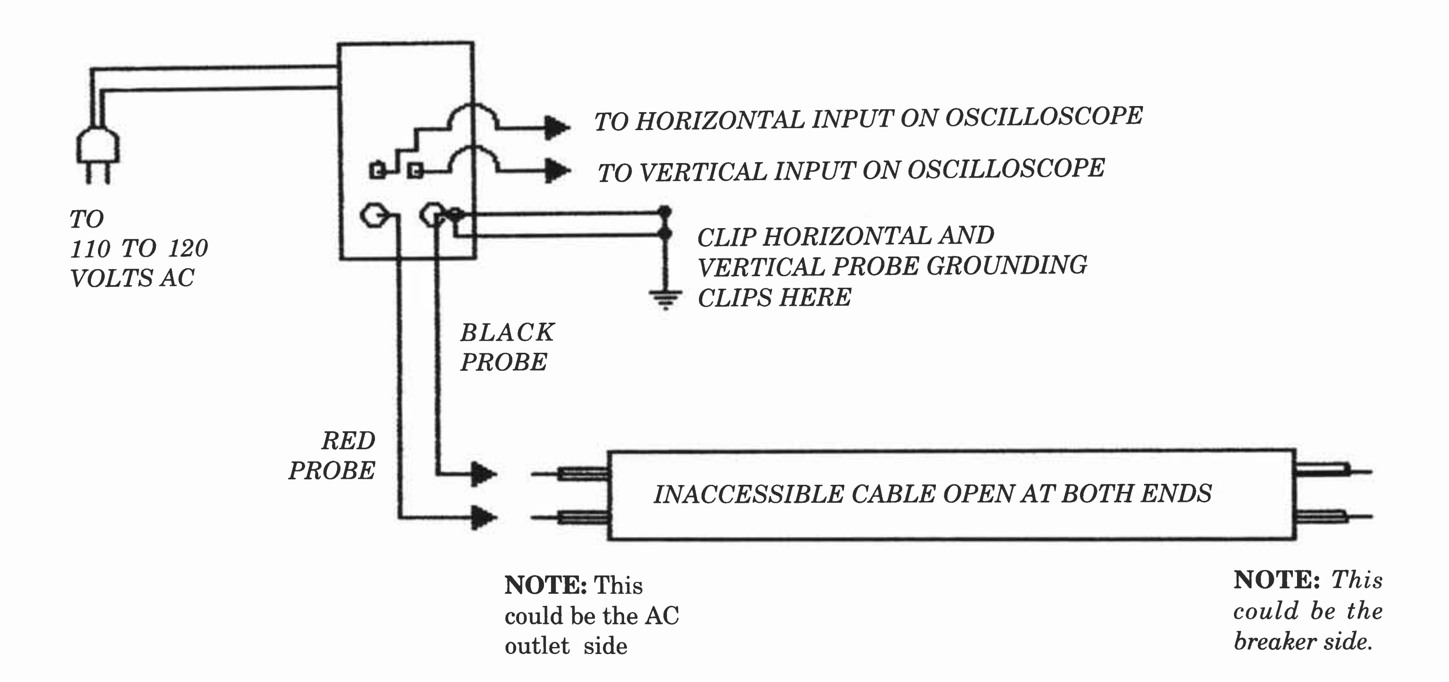
PARTS LIST:

R1 – 10K ohm 5-watt resistor
R2 – 2 Meg 1/2-watt resistor
R3 – 3.3K ohm 1/2-watt resistor
R4 – 100K ohm 1/2-watt resistor
T1 – 120 volts AC to 12 volts AC step-down transformer
MISC. – AC line cord, terminals, plastic housing, and test probes
F1 – 1-amp fuse for additional safety

CAUTION: WHEN ANALYZING AN AC WIRE PAIR, BE SURE THAT THE CIRCUIT BREAKER FOR THAT PAIR IS SWITCHED OFF.

OPERATIONAL NOTES: All appliances (devices), e.g., light bulbs, etc., should be disconnected from the circuit under test. You must have a cable that is open at both ends! Any device that is still connected to the AC line will give an erroneous reading. Try reading different devices, such as radios, TVs, light bulbs, even a parallel telephone wire tap or two.

POOR MAN'S COMPONENT SIGNATURE ANALYZER



OPERATIONAL NOTES: There is no need to disconnect the wire from the breaker (or fuse) panel. Just turn the breaker to the off position. Be sure to disconnect all appliances, lighting (light bulbs unscrewed), etc.

If this is being used on an inaccessible phone wire pair, you must disconnect the phone pair from the surge protector or key system unit and make sure that all devices (modems, phones, fax machines, answering machines, etc.) are disconnected from the phone line.

Many parallel connected devices will show up on the oscilloscope screen. This is especially true with AC circuits; carrier current transmitters, video transmitter power supplies, and AC-powered surveillance devices will stick out like a sore thumb.

NOTE: The main purpose of this device is to find remotely shut-off surveillance devices connected to the AC power line.

POOR MAN'S COMPONENT SIGNATURE ANALYZER (CONTINUED)



100 feet of phone cable open at both ends.



Self-powered H-Z parallel RF tap on 100 feet of phone cable, open at both ends.



Automatic tape starter connected to 100 feet of phone cable.



Signature of modern infinity transmitter on 100 feet of phone cable, open at both ends.



Signature of condenser microphone connected to 100 feet of phone cable.



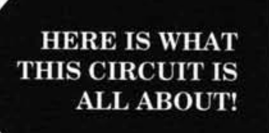
Hidden video surveillance camera power supply connected to 400 feet of AC line with breaker shut off and appliances unplugged and light bulbs unscrewed. Well switches left on an fluorescent ballasts should be disconnected.



Signature of carrier current transmitter connected to 400 feet of AC line. Breaker turned off, appliances unplugged, light bulbs unscrewed, and fluorescent ballasts disconnected.



*Signature of carrier current transmitter **turned off** and connected to 400 feet of AC line with breaker shut off, appliances unplugged, light bulbs unscrewed, and fluorescent ballasts disconnected.*



NOTE: It would be a good idea to take your own baseline readings and make your own charts.

POOR MAN'S COMPONENT SIGNATURE ANALYSIS CHARTS

INCENDIARY DESTRUCTION OF INACCESSIBLE TAPS AND LINE-CONNECTED BUGS

After looking at the diagram for this device, it should be readily apparent what it is used for: reducing little bitty buggies and tappies to burnt-out cinders!

Many years ago I did some experiments using a neon sign transformer and some parallel connected telephone taps. I hooked these taps one at a time to a 100-foot piece of phone cable attached to the high-voltage terminals of a neon sign transformer. Much to my dismay, I would occasionally run across the proverbial "tough nut to crack," a tap that could withstand a repeated 12,000-volt surge. But I'm glad to report that most of the taps were fried to a crisp (electronically speaking)!

These high-voltage transformers can kill you if you are not careful! When this device is used, it should be connected to a cable that is disconnected at both ends and not shorted! Do not even try to connect this device to the telephone company side of the line; the phone company has plenty of spike protection on its lines, including your own surge protector on the outside of your house.

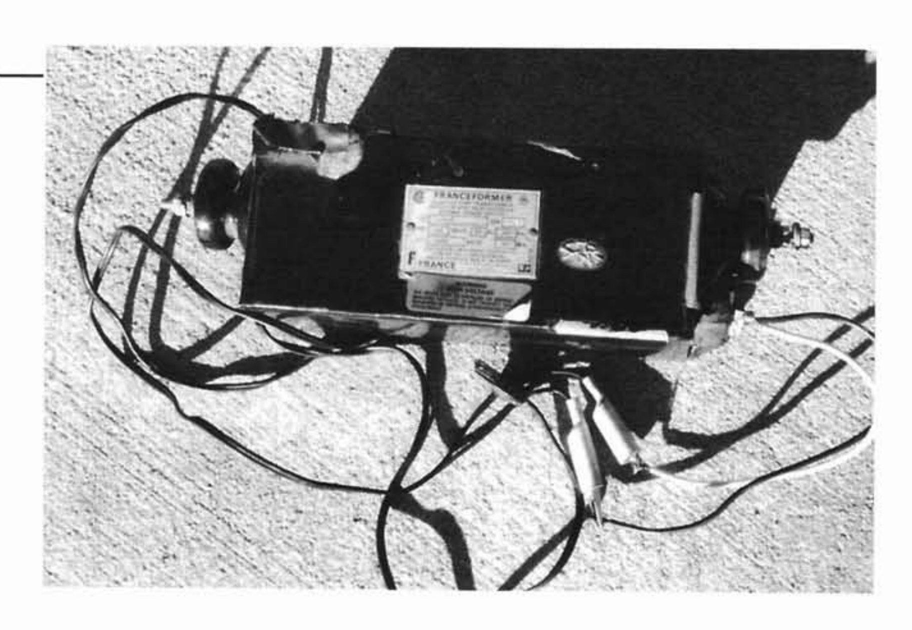
This device can be used with power lines in the house as long as the following precautions are observed:

1) Make sure that the breaker for the circuit undergoing this technique is shut off.
2) Make double sure with your meter and/or neon circuit tester that there is no voltage on the line.
3) Make absolutely sure that all appliances, doorbell transformers, lamp dimmers, lamps, and so on are disconnected from the power line.

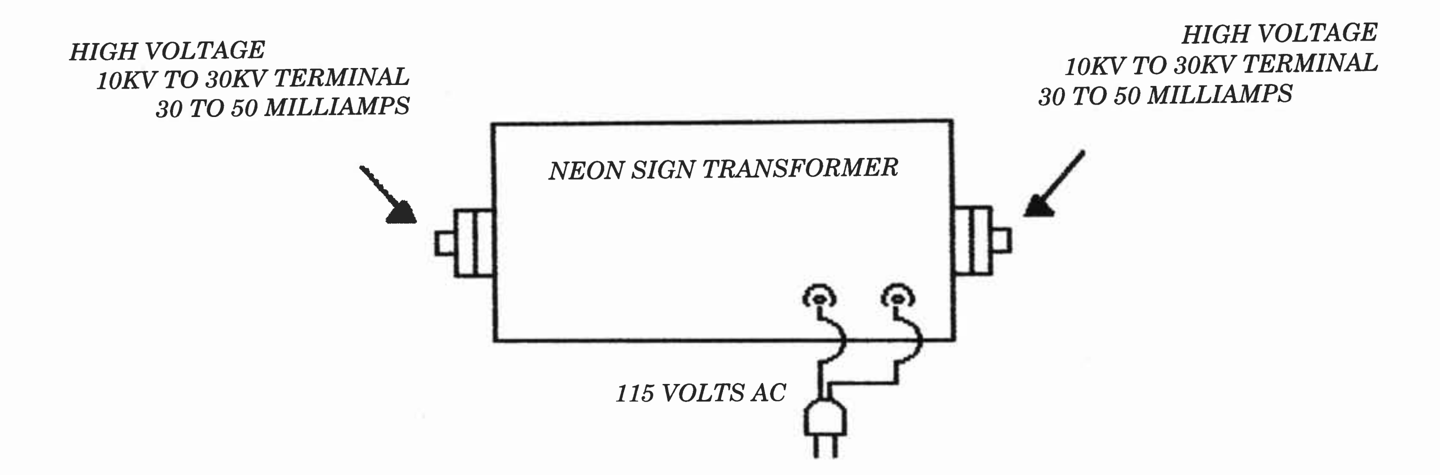
If you use this device on an interior phone line circuit, make sure that the telephone line is disconnected from the surge protector and that all telephones, fax machines, answering machines, modems, and so on are unplugged from their respective RJ11 phone jacks.

WARNING: Please be aware that this technique poses an extreme fire hazard! Stay on the premises for a while with a fire extinguisher after you are all done using the neon sign transformer.

One time I started a fire in a telephone jack (RJ11); yuck, nothing like the smell of burning plastic in the morning! The contacts on the modern telephone jacks are very closely spaced, so some arcing will occur.



Neon sign transformer with 120-volt AC primary and 12,000-volt secondary at 30 milliamps. This will "fry" most inaccessible parallel-connected bugging and tapping equipment. Be very careful with this, i.e., make sure that the cable (power or phone line) that the device is connected to is disconnected (open) at both ends!



APPLICATION NOTES: Connect high-voltage terminals to an inaccessible wire pair. Make sure that the inaccessible wire pair is disconnected at both ends. If phone lines are being cleared, make sure that phones, fax machines, answering machines, and such are disconnected. If AC wiring is being cleared, make sure that appliances are disconnected and that *the breaker is shut off*. For series-connected devices, one end of the cable should be shorted.

WARNING: Failure to follow the procedure listed above could result in serious damage to equipment and appliances connected to the line and could result in serious damage to the premises and the technician! Some countermeasures technicians have been known to connect this device to the phone line in order to destroy off-premises telephone taps. Any attempt to destroy off-premises taps could result in damage to phone company equipment and very angry telephone security personnel! *Internal phone wiring should be disconnected from the surge protector. The surge protector, if left connected, would dissipate much of the high-voltage charge.*

FIELD OBSERVATIONS: Using a 12KV (12,000-volt), 30-milliamp neon transformer on internal telephone wiring disconnected from the surge protector, I observed the following: *arcing in the telephone jack due to the very close spacing of the terminals, which resulted in a small fire!*

INCENDIARY DESTRUCTION OF INACCESSIBLE TAPS AND LINE-CONNECTED BUGS

NO-BRAINER PHONE LINE SENTRY
(THIS WILL TELL YOU IF YOUR PHONE LINE WAS TAMPERED WITH!)

I came up with this idea back in the early 1980s, quite by accident. One day when I was testing an automatic tape starter, I left my house for a few hours to run an errand, and when I got back I was treated to a couple of rather long-winded personal conversations between a telephone company lineman and both his girlfriend and his central office.

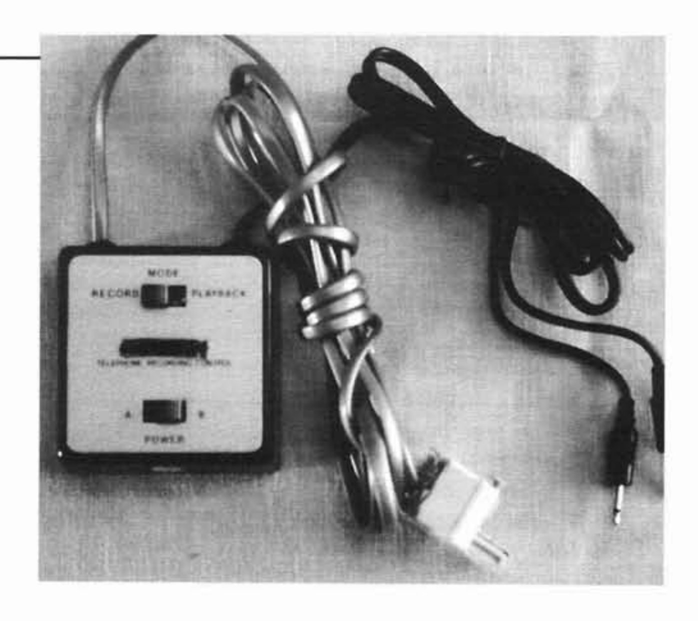
At this point, the proverbial light bulb went off in my head: what a great way to tell if some telephone tapper/bugger was testing and tampering with your phone line!

The reason for the "No-Brainer" in the title of this project is simple: it uses a goof-proof automatic tape recorder starter that's very easy to obtain and use connected to a cheap, readily available tape recorder (with a remote jack).

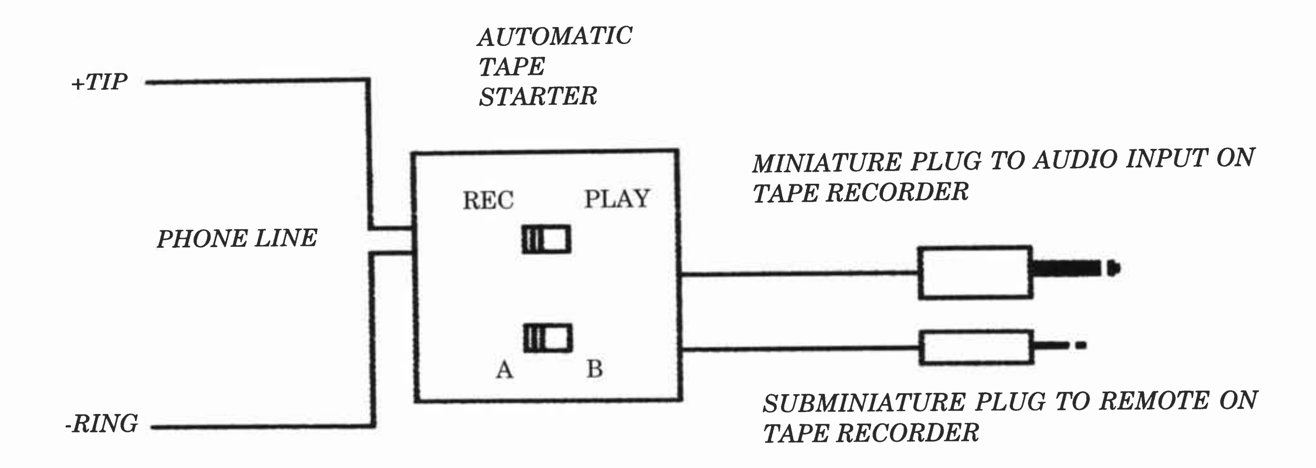
If you need this apparatus to be concealed, then just plug it into a phone jack that is located behind a large cabinet or pile of junk.

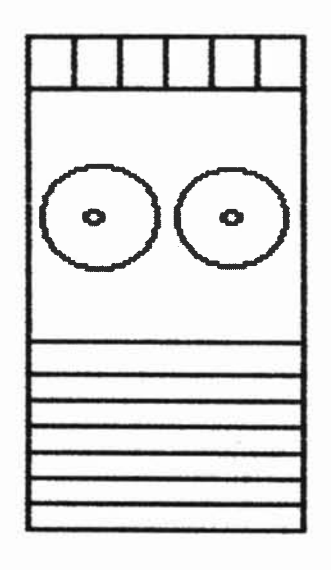
If you need to be a little more covert, try the following: cut off the male plug on the automatic tape starter and connect alligator clips, which are then connected to the phone line in a hidden location where the phone lines run (i.e., the basement or attic).

Be sure to follow the instructions that come with the automatic tape starter. A and B selector switch is a polarity adjustment switch. Be sure to select the REC (record) mode. If you record other people's conversations (who share or visit your premises), you must erase and not play back their private conversations according to the law.



No-brainer phone line sentry. Just add a tape recorder with a remote jack and a tape counter and you will have a "goof proof" watchman for your phone line! Be sure to read the privacy laws regarding the use of this system.





NOTE: Automatic tape starters are available at Radio Shack and most large, full-line electronic supply companies. Most come equipped with modular connectors. If you need to hide this unit, just cut off the modular end and attach alligator clips.

CHEAP TAPE RECORDER WITH REMOTE JACK

NO-BRAINER PHONE LINE SENTRY

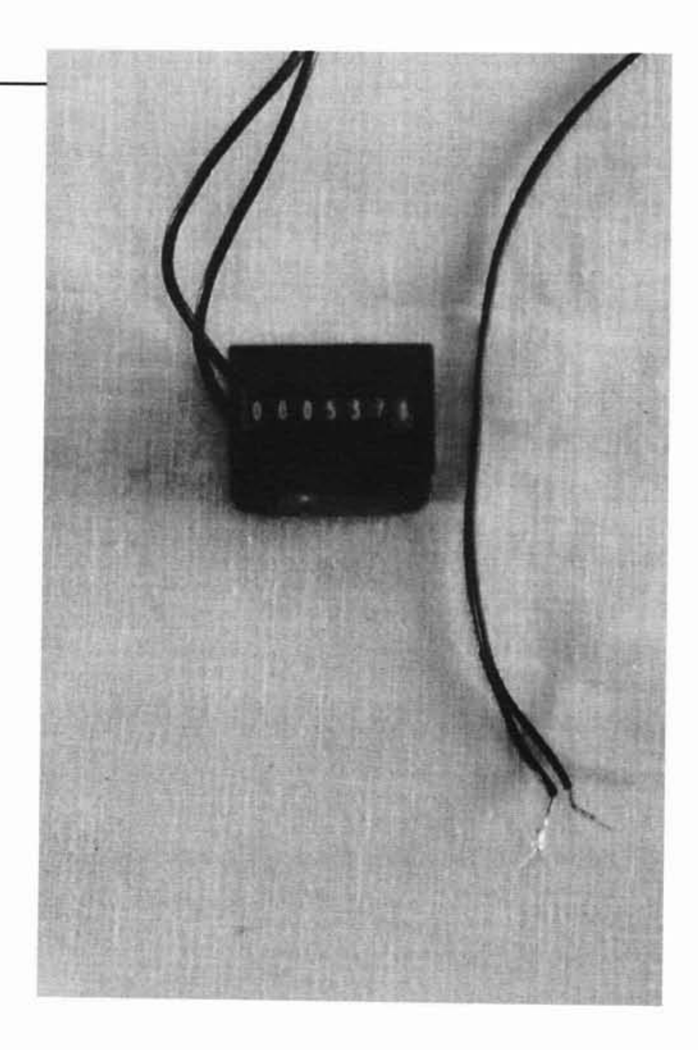
PHONE LINE USAGE AND CUT MONITOR

This is an unusual twist on the various phone line cut and usage monitors I have seen over the years. This circuit has a very high impedance input (80 megohms resistance) and a counter to keep track of the number of times the phone is lifted from its cradle or how many times the phone line has been cut and then reconnected.

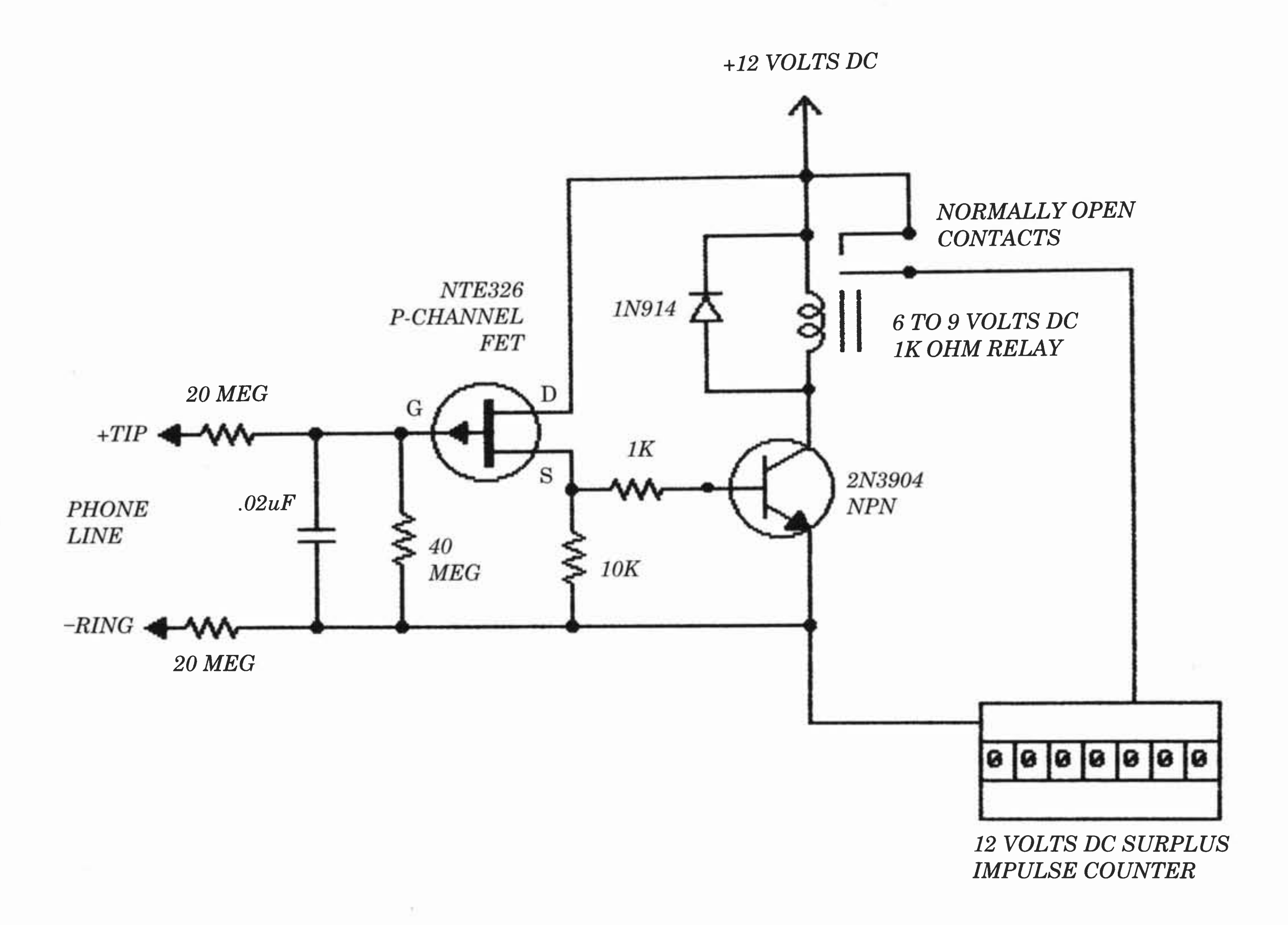
A temporary phone line cut can indicate an installation of a series telephone tap. If there is an indication that the phone was taken off the hook a number of times when nobody was home, it may suggest tapping, bugging, and testing.

Take a look at the circuit. When a phone is lifted from the cradle or a lineman's test set is used or a phone line cut occurs, the FET transistor triggers on the drop in voltage (48 to 7 is typical). The FET transistor turns on, thereby making the base of the NPN transistor positive. With the NPN transistor turned on, current will flow through the relay, thereby energizing the impulse counter, giving us a half count. When the phone line is reconnected or when the phone goes back in the cradle or the operative is done making his test call, the FET transistor turns off and in the process turns off the NPN transistor, which turns off the relay. The impulse counter is now de-energized, giving us the remaining half count, which will then give us one full count.

The .02 capacitor prevents false triggering from the AC ringing voltage, and it also lowers the AC impedance of the circuit to slightly over 40 megohms, depending on the frequency of the test signal.



A low-tech solution for determining how many security breaches occurred. Here is the 12-volt DC impulse counter, which is used for several projects in this book. These nonresettable counters are a great way to count how many times a violation (event) occurred.



NOTE: All resistors are 1/4-watt, .02uF capacitor, 200 to 300 volts DC.

APPLICATION NOTES: This is almost identical to the 80-megohm automatic tape starter circuit. The impulse counter is the same unit that was used in my original book on this subject, *Bench-Tested Circuits for Surveillance and Countersurveillance Technicians.* When the phone is picked up and then hung up, one full count will be registered. When a lineman's test set is used or the phone line is *temporarily* disconnected or cut, a full count will be registered.

SEQUENCE:

PHONE PICKED UP GIVES 1/2 COUNT

PHONE HUNG UP GIVES 1/2 COUNT

THIS RESULTS IN ONE FULL COUNT

PHONE LINE USAGE AND CUT MONITOR

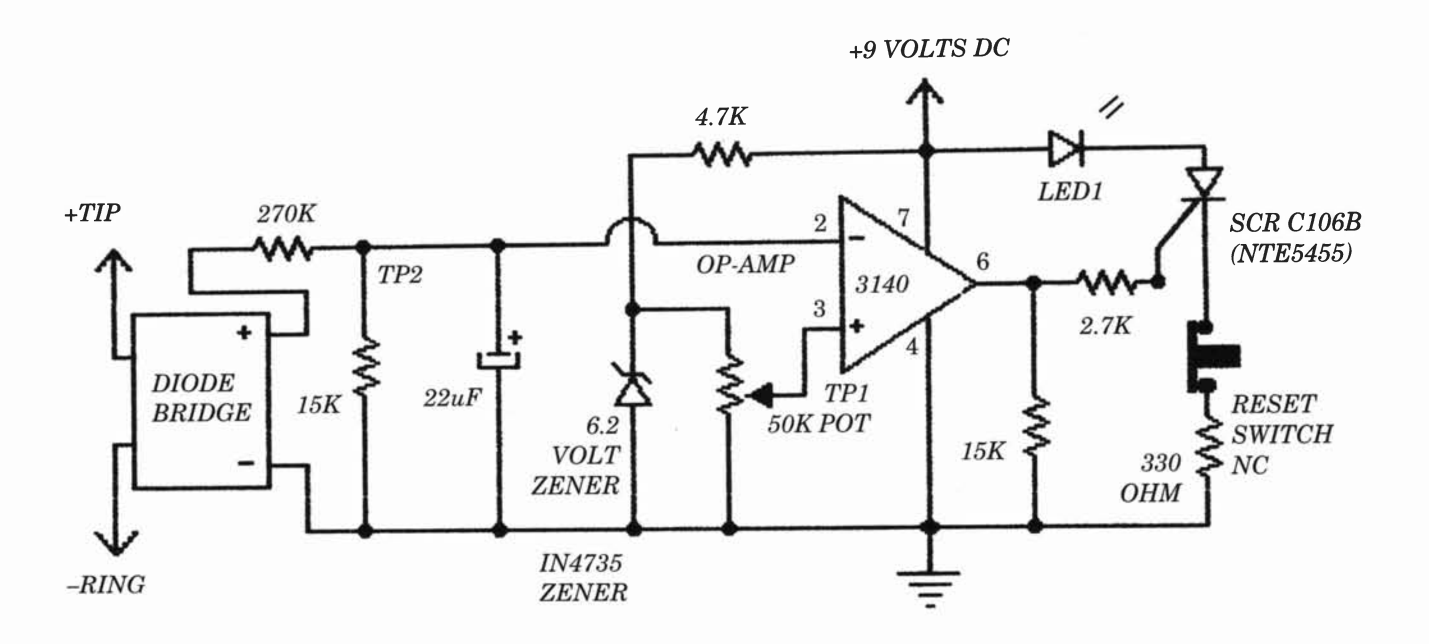
PHONE LINE USAGE AND CUT MONITOR WITH VARIABLE-VOLTAGE TRIP POINTS

This circuit can be set for various voltage trip points, i.e., one phone off the hook, two phones off the hook, etc. It can also be set for a line cut. It will be absolutely necessary to adjust the 50K potentiometer, which can be a little tricky at times and must be done on the phone line in question. Let's take a look at the circuit.

The 3140 op-amp functions as a comparator. I decided on the 3140 because it is a high-performance FET input type. The 270K resistor gives us fairly good isolation from the phone line, and it also forms a voltage divider with 15K resistor. With the 50K potentiometer set properly, the phone is taken off the hook. There is a drop in voltage at pin 2 (inverting input), which now falls below the reference voltage set by the wiper on the 50K potentiometer. At this point pin 6 (output) goes high, triggering the sensitive gate SCR. The SCR latches LED1 on. In order to turn off the LED, it must be turned off via the normally closed reset switch. The 6.2-volt zener diode keeps the reference voltage stable.

WARNING: Do not omit the 22uF capacitor—it prevents false triggering caused by the AC ring voltage.

NOTE: An AC-to-DC adapter can be used to replace the 9-volt battery for long-term use.



NOTES:
All resistors are 1/4-watt.
Op-amp – CA3140 (FET input)
The 50K ohm potentiometer controls the voltage trip point
SCR is a sensitive gate type
The 22uF capacitor prevents false triggering (do not omit)!
Diode bridge – 200 volts minimum rating.

IMPORTANT: Readings will vary due to component tolerances, construction practices, and the large variety of phone equipment available. Be sure to thoroughly test your phone equipment with this circuit before you depend on it to protect you!

ACTUAL TEST CASE WITH AN OLD 2500 SERIES TOUCH TONE PHONE:
(Measurements made with a 20-megohm DVM)

With the wiper (TP1) set at 250 millivolts with respect to ground and 2.5 volts from (TP2) to ground, the LED triggered when the phone was lifted from the cradle.

With the wiper (TP1) set at 60 millivolts with respect to ground and 2.5 volts from (TP2) to ground, the LED triggered only when the phone line voltage dipped below 1.5 volts.

PHONE LINE USAGE AND CUT MONITOR WITH VARIABLE-VOLTAGE TRIP POINTS

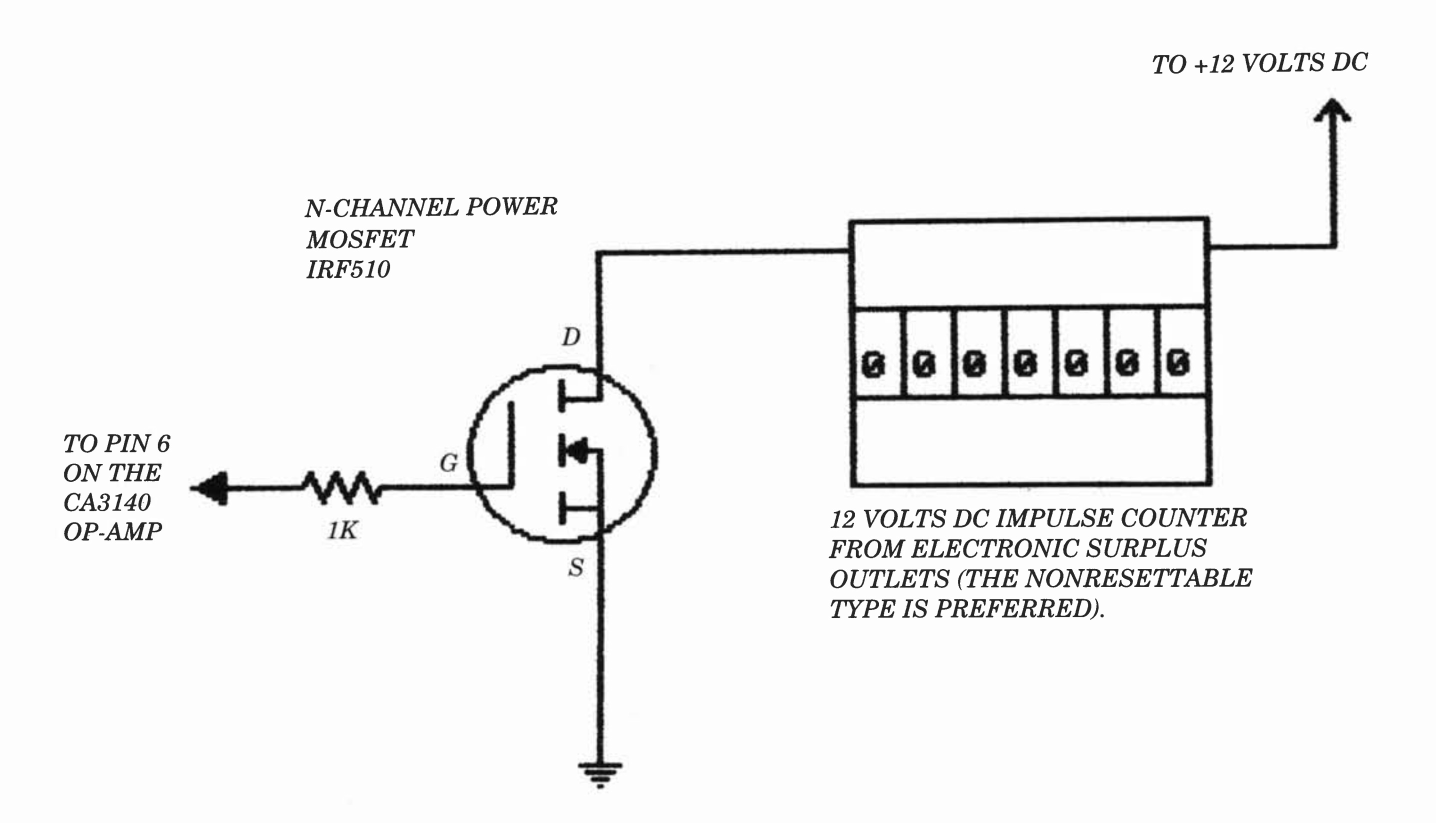
OPTION FOR PHONE LINE USAGE AND CUT MONITOR WITH VARIABLE-VOLTAGE TRIP POINTS

With this circuit you would eliminate LED1, the 2.7K resistor, the 330-ohm resistor, the reset switch, and the SCR in the circuit that preceded this one.

About the circuit (refer to the original schematic on p. 13): When pin 6 goes high (in the original circuit), the N-channel power Mosfet starts to conduct, thereby energizing the impulse counter. The impulse counter stays at one-half count until pin 6 (in the original circuit) goes low. Once pin 6 goes back to a low state, the counter gives a one-digit count.

The IRF510 (refer to the schematic) was chosen for its power handling capabilities and its "very low on-state resistance." Most of the "surplus" impulse counters for DC voltage applications that I have personally seen are of the 12-volt DC variety. The counter I used had a 52-ohm resistance, which will draw 231 milliamps in an energized state. An AC-to-DC adapter would not be a bad idea for this circuit; in fact, it could also run the previous circuit.

The real beauty of this circuit is the fact that you can now find out how many times an event occurred! You could have two of these systems on a given phone line set to different trip points—one for line cuts and one for telephone usage (and testing by the operatives).



NOTE: This circuit replaces the SCR, LED1, normally closed reset switch and the 330-ohm resistor in the original circuit. The 2.7K resistor has been replaced with a 1K resistor. The 9-volt battery has been replaced with a 12-volt battery in order to operate the impulse counter.

APPLICATION NOTES: When the trip point is set for handset-off-hook triggering, one full count will take place when the handset is lifted and then set down on the cradle (thus, one-half count when the handset is lifted and one-half count when the phone is hung up). When the trip point is set for line-cut-only mode, one full count takes place when the line is cut and then reconnected.

OPTION FOR THE PHONE LINE USAGE AND CUT MONITOR WITH VARIABLE-VOLTAGE TRIP POINTS

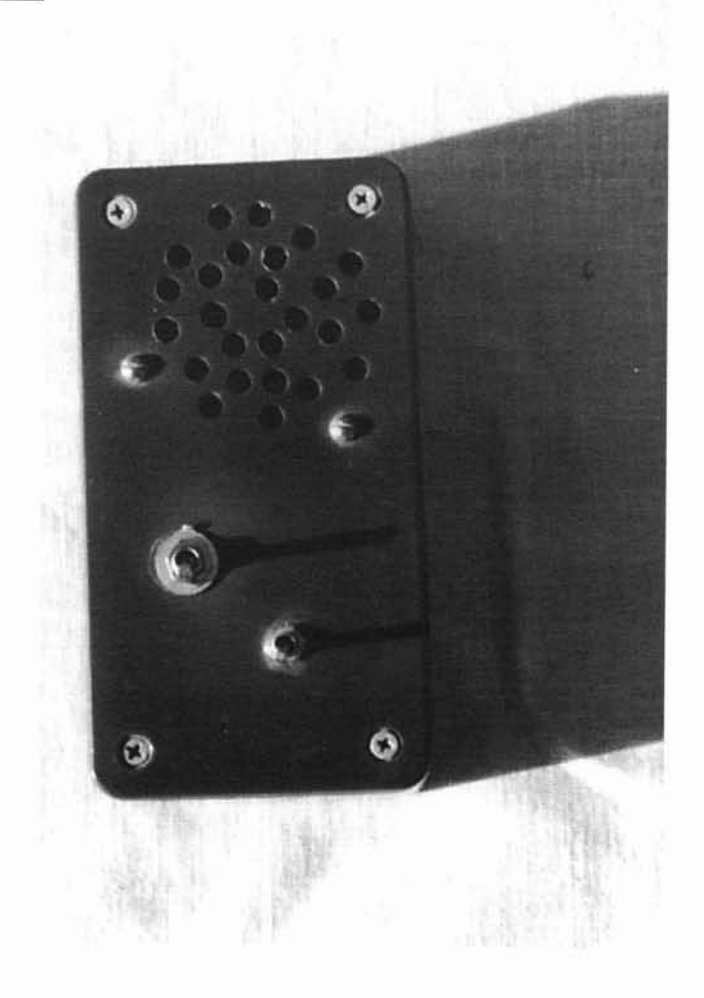
SIMPLE TELEPHONE ISOLATION CIRCUIT

This circuit stops most conventional telephone bugging techniques I know of. It obviously will not stop an inside-the-telephone-instrument type of tap or a self-powered (battery-operated) bugging transmitter hidden inside the telephone set for convenience. It does tend to stop every kind of hookswitch bypass and line-powered amplifiers hidden in the telephone set. It will also stop the very clever "custom-built" telephones equipped with on-board (modern) infinity line transmitters that get around the ESS systems. Let's take a look at the circuit.

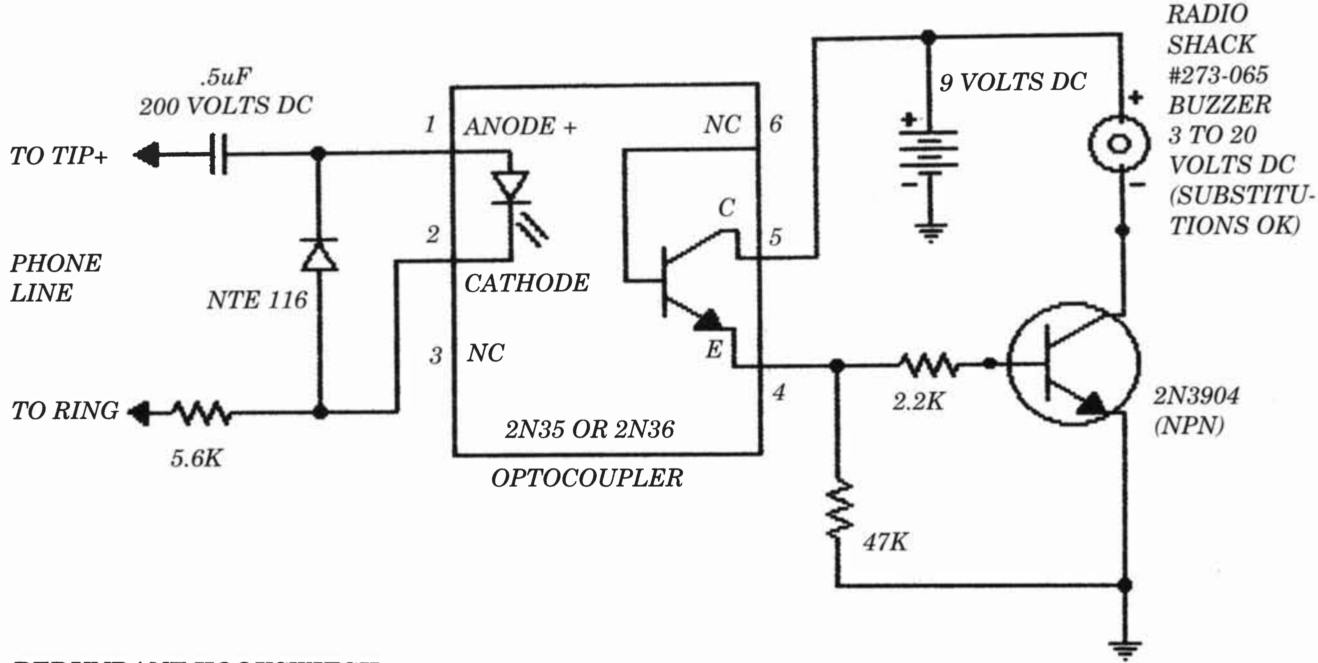
The first section is the telephone ring detector circuit called the "substitute ringer section." At this point I think it's only fair to mention the fact that you could buy an "off-the-shelf" ringer from a telecommunications supplier or even a hardware store. You don't even have to go along with my design; there are plenty of telephone ringer circuits in various electronic magazines and books. The redundant hookswitch (for lack of a better term) is just a simple double-pole single throw (DPST) switch. This DPST switch completely isolates the telephone set from the phone line. When the substitute ringer sounds off, you would throw the DPST switch and answer the phone. When you need to call out, just turn the DPST switch to the "on" position and make your call.

IMPORTANT: Don't forget to turn the DPST switch to the off position when you are done using the phone!

I recycled an old plastic project box for the "Simple Telephone Isolation Circuit." The extra switch is for "DO NOT DISTURB." It turns off the substitute ringer. Bugging the phone instrument will be impossible with this device, so long as the circuit inside the box is not bypassed. Cover the screws with paint or glue to avoid tampering or bypassing.



SUBSTITUTE RINGER SECTION:

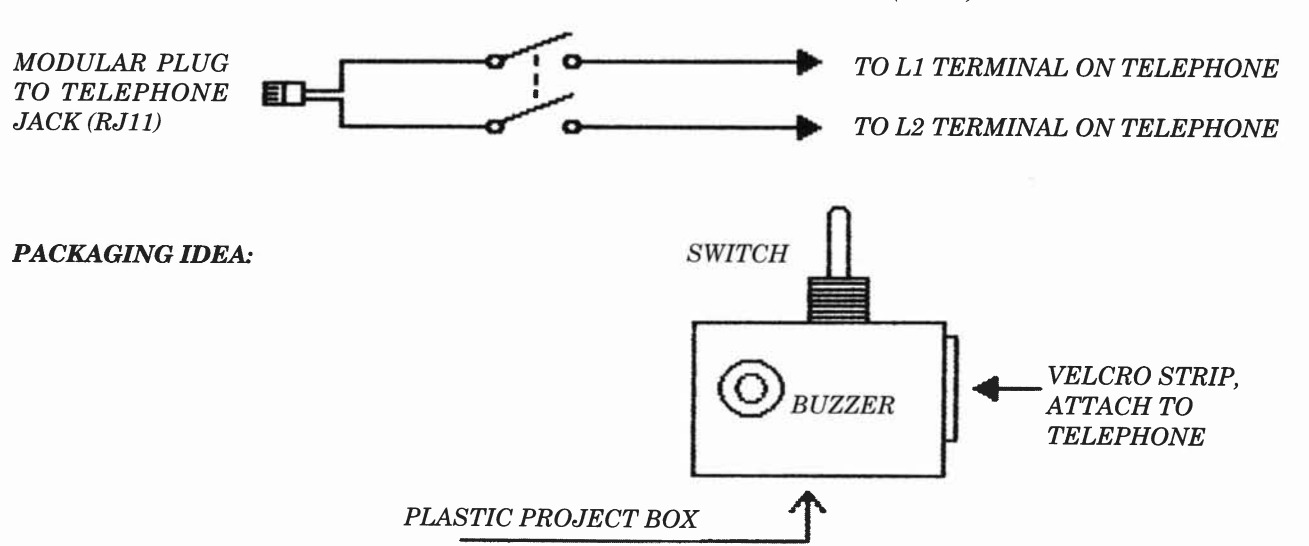


REDUNDANT HOOKSWITCH:

DOUBLE POLE SINGLE THROW SWITCH (DPST)



PACKAGING IDEA:



SEQUENCE:

1. BUZZER SOUNDS (PHONE CALL)
2. THROW THE DPST SWITCH
3. ANSWER PHONE

APPLICATION NOTE: This will stop most telephone instrument bugging, such as hookswitch bypass modifications and inside-the-phone "leach" type transmitters.

SIMPLE TELEPHONE ISOLATION CIRCUIT

PROXIMITY DETECTOR

Several years ago, I needed a circuit that could turn on a device when a person came within three feet of a protected object. A further requirement was that it needed to stay on until the person left the three-foot protection zone around the object.

Passive Infrared Detectors (PIRs) only filled half the requirement. PIRs only detect "heat in motion"; when a person enters a protected area, the PIR trips an alarm. However, *a PIR will not tell you the current status of the protection zone*. The following question remains: is the person still in the protection zone or not? If the person stays motionless in the protection zone, the PIR *will not detect a presence!* One of the requirements of a PIR is that you have motion. If you have no motion, then obviously you have no detection! PIRs can also be fooled very easily (more about that in another book).

The following circuit overcomes the inherent problems with PIRs. It is a basic *capacitor effect relay*. When a person steps into the protected zone of the sensor (nothing more than an antenna or a piece of metal), the relay activates an external circuit, and it stays on until that person leaves the protected zone.

This simple yet very powerful circuit has very useful applications for monitoring the current status of a secured area, or as simple an application as turning on a reading lamp when someone enters a room and then turning it off when the person leaves the room.

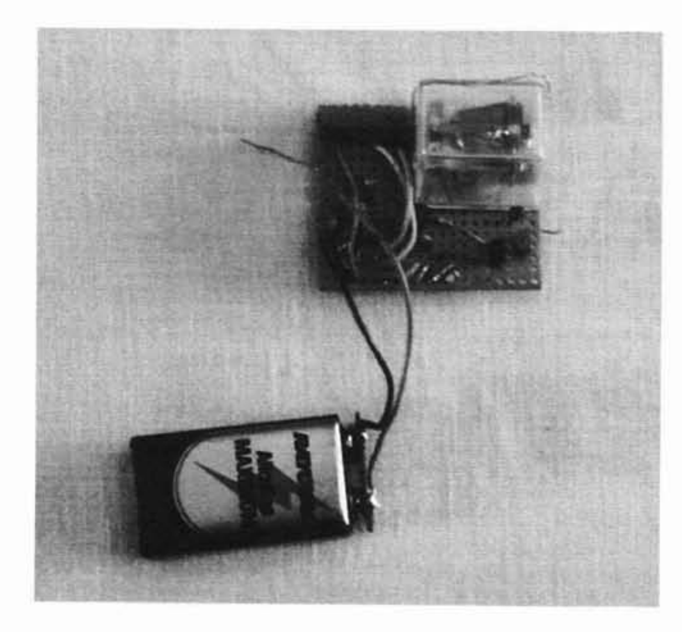
Here is how it works.

The colpitts oscillator operating at close to 150kHz is adjusted via R4 to a point where the oscillations are just barely sustained. The sensor (which could be a large metal desk, door knob, piece of wire or vehicle, etc.) is an important part of the oscillator section. If someone gets too close to the sensor, the oscillations will cease. This turns off transistor Q3, which makes the base of Q4 positive and in turn energizes the relay. Q2 acts as a buffer and diodes D1 and D2 provide rectification for the output of the oscillator buffer (Q2). LED1 is helpful when adjusting R4, the sensitivity control (also known as an oscillator adjustment control).

Important "real world" application notes:

This circuit should have a good earth ground, i.e., earth, water pipe, or an electrical system ground. The screw on an electrical outlet or switch plate will do if the building is properly grounded. You can easily check to see if the electrical system is grounded just by reading the voltage between hot and ground. It should read almost the same voltage as hot to neutral.

I would strongly suggest the use of an oscilloscope with the probes connected to Q1's collector and ground (with the probe in the x10 position). Connect one end of a piece of wire to C4 and the other end to a piece of metal (anything from a door knob to a screen door). Adjust R4 to a point just above where the oscillations cease. The closer the setting, the more sensitivity you will obtain. R4 should be a good quality, multiturn potentiometer. I would strongly recommend the optional voltage regulator circuit or, better yet, an AC-to-DC power adapter, or you may find yourself re-adjusting this circuit on a daily basis.



Here is the completed "Proximity Detector" minus the voltage regulator circuit.



PARTS LIST:

IC1 – 317T adj. voltage regulator (optional)
Q1, Q2, Q3, Q4 – 2N2222 or 2N3904 NPN transistors
R1, R2 – 56K ohm 1/8-watt resistors
R3 – 2,800 ohm 1/8-watt resistor
R4 – 5K miniature multiturn linear potentiometer
R5 – 3,300 ohm 1/8-watt resistor
R6 – 33K ohm 1/8-watt resistor
R7 – 2,200 ohm 1/8-watt resistor
R8 – 6,800 ohm 1/8-watt 1/8-watt resistior
C1, C2 – 470pF capacitors
C3, C6 – .01uF capacitors
C4 – .001 uF capacitor
C5, C7 – .1uF capacitors
L1 – 2MH (millihenry)
D1, D2, D3 – 1N914 silicon diodes
LED1 – red light emitting diode
K1 – 500 ohm, 6- to 9-VOLT DC RELAY
SENSOR – see text

PROXIMITY DETECTOR

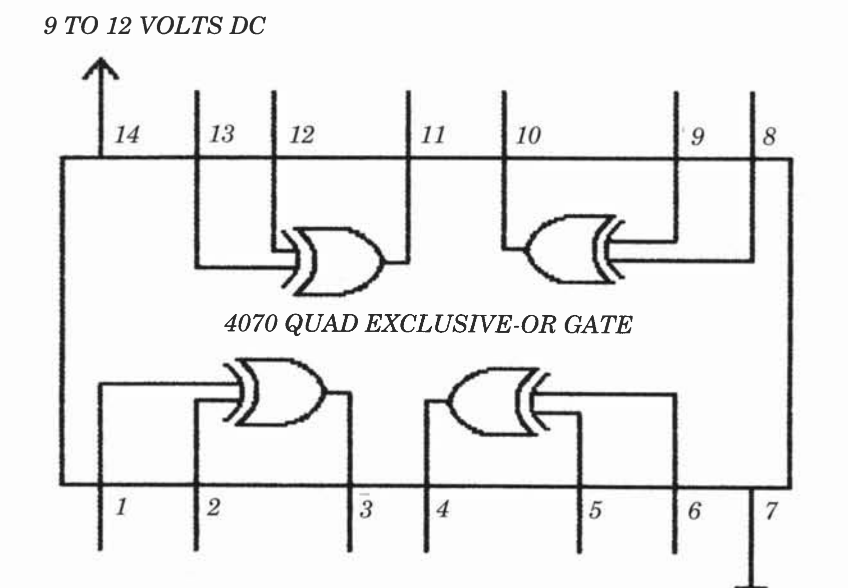
AUDIO INTRUSION ALARM SYSTEM

Back in the early 1980s I was reading a brief synopsis of various alarm systems. I read with great interest a two-paragraph description of an audio intrusion alarm system. Some time later when I was reading a digital logic handbook, I stumbled upon a description and truth table for a quad exclusive-OR gate.

At that point, I flashed back on the brief synopsis of the audio intrusion alarm, and it came to me: “This must be the heart of this unique alarm system!” I then reasoned that the rest of the system would consist of two microphones, two amplifiers (located in different parts of the building and adjusted for the ambient noise characteristics), two simple AC-to-(boosted) DC signal processors, and some sort of alerting or latching system. Let’s take a look at the circuit.

The output of the amplifiers is boosted by T1 and T2 and then rectified by the diode bridges. R1, R2, C1, and C2 act as a time delay and filter for the rectified signal.

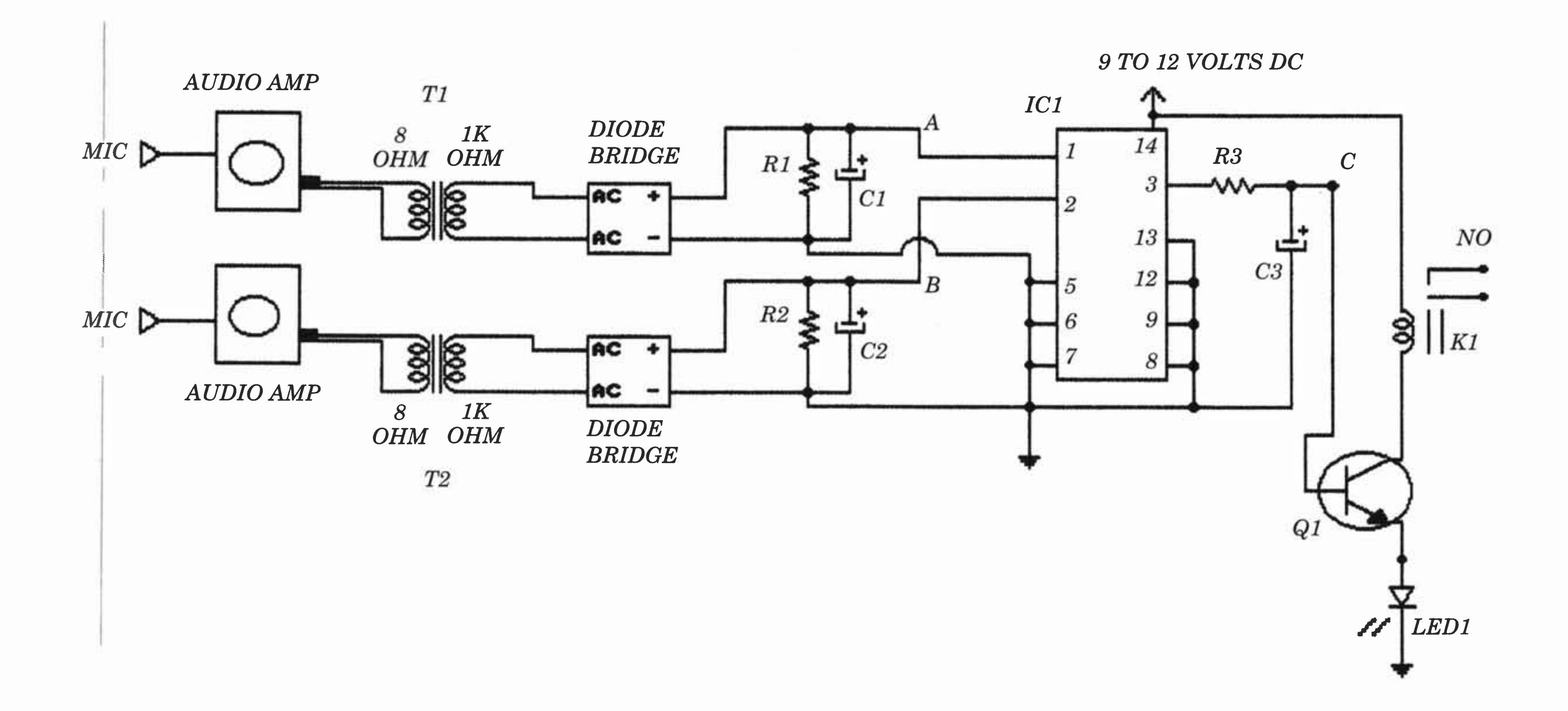
When lightning strikes outside, the sound will be amplified and processed and will give us a high at both inputs (1 and 2) of IC1. According to the truth table, a high at both inputs will give us a low at the output, pin 3. With a low at pin 3, transistor Q1 will not conduct, and as a result will not energize the relay or LED1. When all is quiet we have a low at both inputs (1 and 2), and according to the truth table we consequently have a low at pin 3 of IC1, and Q1 will still not conduct. When the sound of a break-in occurs at the first microphone, we get a high at pin 1, a low at pin 2, and a high (according to the truth table) at pin 3 of IC1. With a high at pin 3, transistor Q1 turns on and energizes the relay and LED1.



TRUTH TABLE

A	B	OUT
L	L	L
L	H	H
H	L	H
H	H	L

QUAD EXCLUSIVE-OR GATE 4070, PIN OUT



PARTS LIST:

T1, T2 – 8 ohm to 1K ohm miniature audio transformer
DIODE BRIDGES – 100 volt, 1 amp
R1, R2 – 100K ohm 1/4-watt resistors
C1, C2 – 47uF capacitor
R3 – 1,000 ohm 1/4-watt resistor
C3 – 100uF capacitor
AUDIO AMPS – identical amplifiers (I used two shirt pocket-sized Radio Shack amplifiers). Both amps should be set to a loud volume.
IC1 – 4070 quad exclusive-OR gate
Q1 – 2N3904 general purpose NPN transistor
LED1 – red light emitting diode
K1 – 500- to 1,000-ohm, 6- to 9-volt relay
MIC – Make two identical "Remote Condenser Microphones" as outlined in Bench-Tested Circuits for Surveillance and Countersurveillance Technicians (p. 32).

AUDIO INTRUSION ALARM SYSTEM

AUDIO INTRUSION ALARM SYSTEM ENHANCEMENT
(ADD-ON CIRCUIT TO REDUCE FALSE TRIGGERING)

Please refer to the original "Audio Intrusion Alarm System" schematic (p. 21).

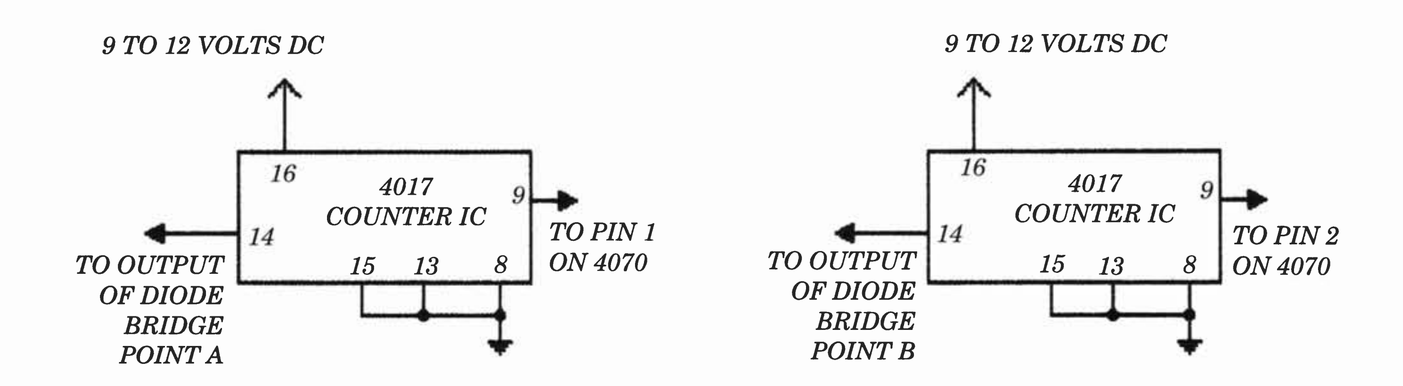
Let's take a look at the circuit.

The 4017 counter IC is configured as a divide-by-nine counter, which simply means nine counts in equals one count out. The 4017 counter IC reduces false triggering, such as a book falling off the shelf, a heavy part falling on the floor, or a random backfire of an engine on one side of the building. This circuit will more than likely have to be tailored to your needs.

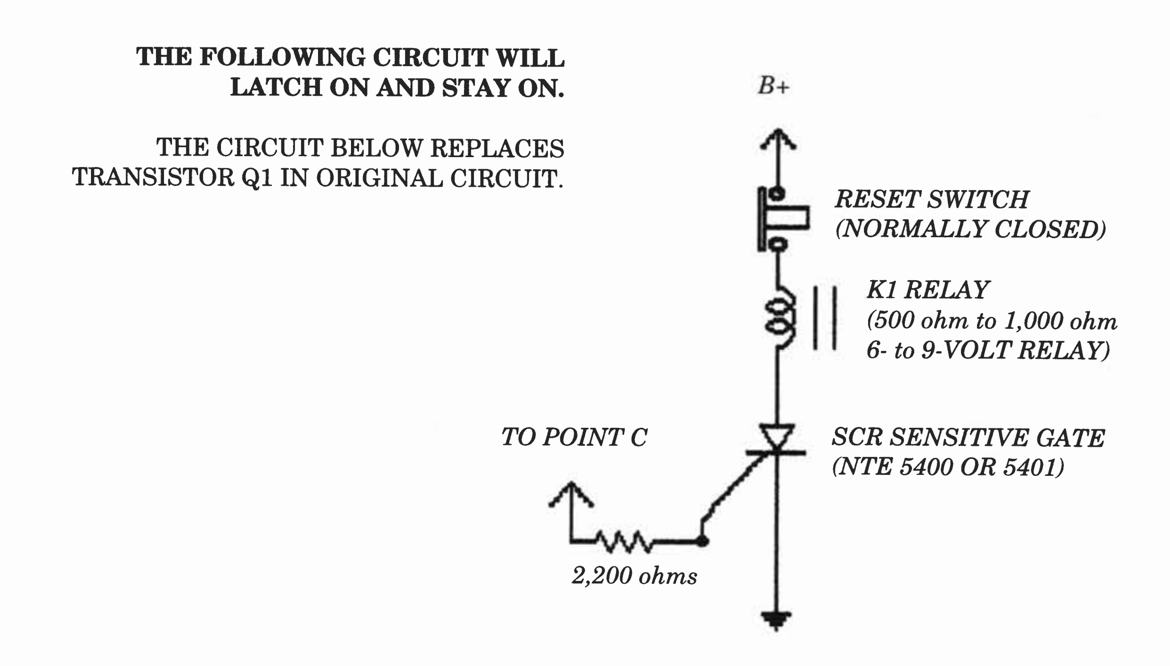
You may find that you need to cascade extra 4017 counter ICs for your particular application, such as two 4017 counters cascaded with the output feeding pin 1 of the 4070 IC and perhaps only one 4017 counter IC feeding pin 2 of the 4070 IC. Don't be afraid to experiment.

If you need to latch the output, then just eliminate Q1 and R3 in the original circuit and replace them with a sensitive gate SCR, a 2.2K resistor, and a reset switch as shown in the enhancement circuit.

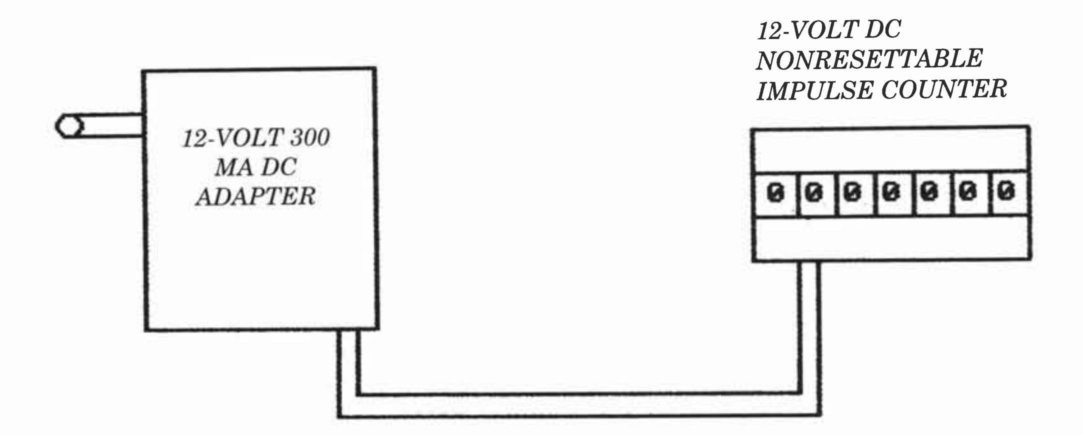
VERY IMPORTANT: I would suggest that you power down the 4017 ICs each time before this alarm system is put into operation. This will reset to zero the 4017 counter ICs. You may or may not have to reset the SCR latching circuit, depending on if there is an output "glitch" or not on power-up. Please bear in mind that this is an experimental, temperamental circuit and results may vary. You may find that you need further signal processing just ahead of the 4017 counter IC enhancements.



NOTE: Refer to the original "Audio Intrusion Alarm System" schematic (p. 21).



AUDIO INTRUSION ALARM SYSTEM ENHANCEMENT



APPLICATION NOTES:
Plug into AC wall outlet of room that needs protection from eavesdropping equipment. Install an identical unit in another nearby "noncritical" room that is on a *separate* breaker. If the critical room registers one+ count or more and the noncritical room that is on a *separate* circuit still registers the original count, then there is a possibility that someone has shut off the breaker to the critical room in order to install an AC-powered bugging device.

INSTALLATION NOTES:
Install units in hidden locations, behind heavy cabinets, etc. You could use a small patch cord with alligator clips on both ends and connect them to the AC lines in the ceiling. Just remove the ceiling tile (or go to the attic if it's installed in a house) and check the counter(s). Always make a note of impulse counter number settings.

IMPORTANT:
When the impulse counter is energized, it will register a half count on the right-hand digit. Just jot down the register count.

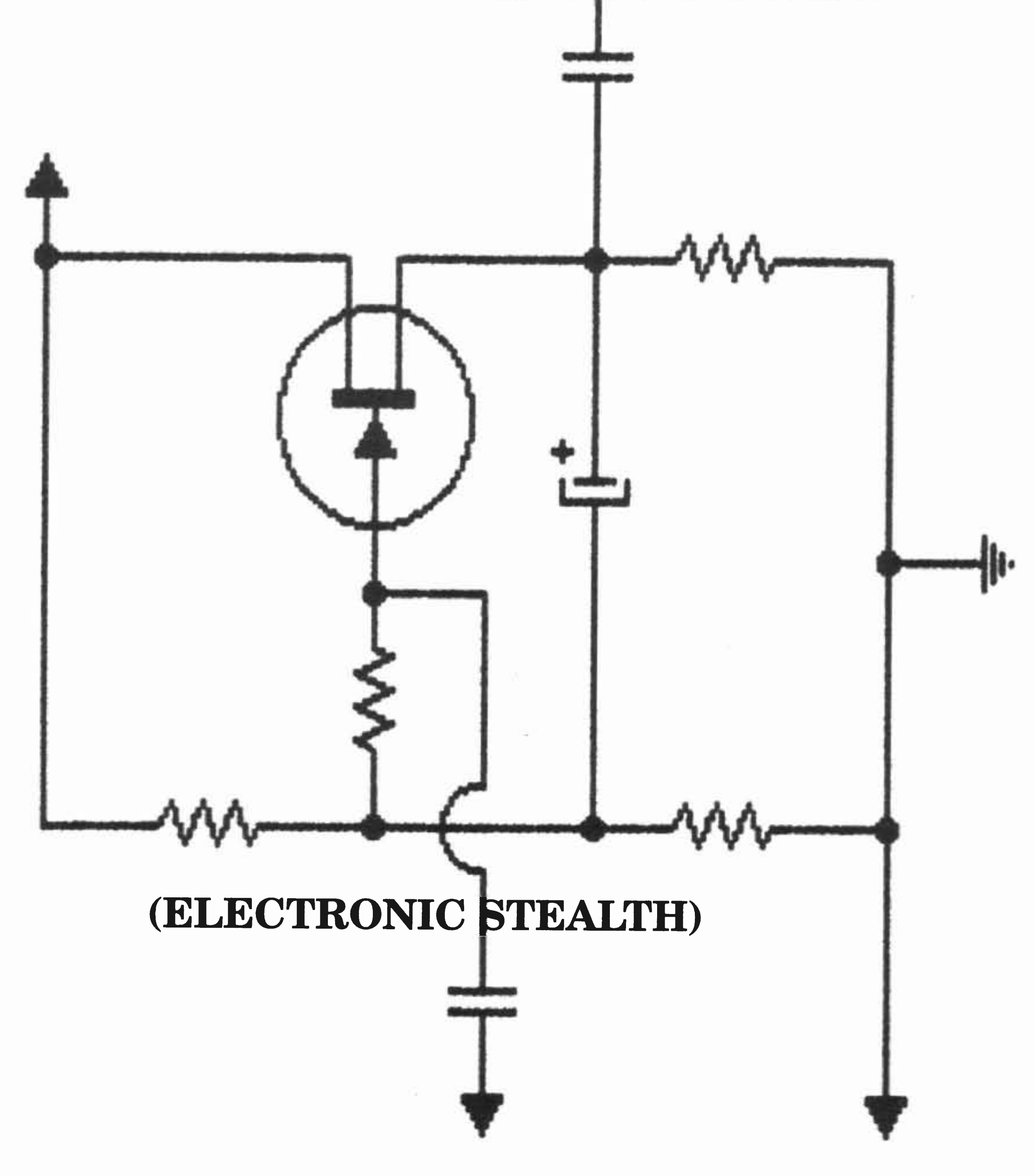
EXAMPLE:



AC VOLTAGE TAMPER ALARM

SECTION II

ELECTRONIC SURVEILLANCE

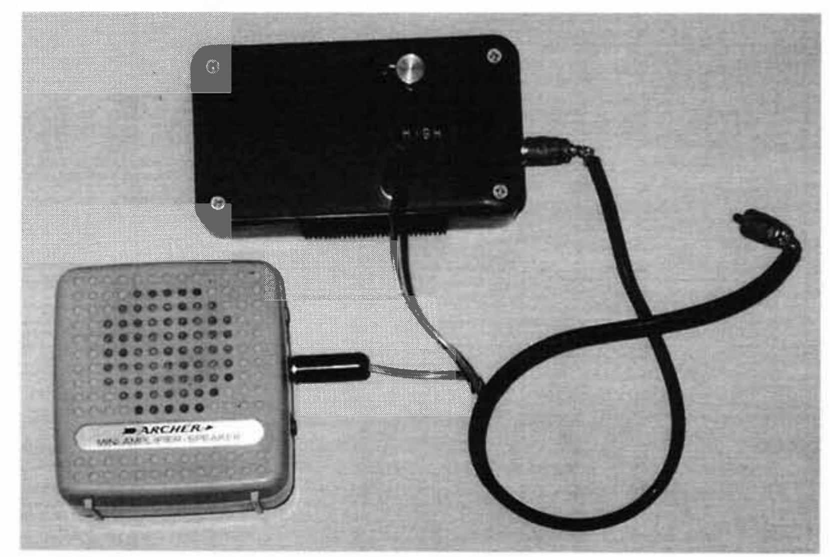


(ELECTRONIC STEALTH)

SCA DECODER
(IT'S GENERIC, BUT IT WORKS)

+ 9 to 12 VOLTS
2K
10K
5K
.001uF
.018uF
.018uF
INPUT
510pF
510pF
.047uF
NE565
PLL
4.7K
1K 1K 1K
4.7K
SCA
OUTPUT
.1uF
4.7K
4.7K
.001uF

OPERATIONAL NOTES: The input is connected to the output of the FM demodulator in a standard FM radio. The de-emphasis circuit may or may not have to be disabled. The output can be connected to the input of almost any general-purpose amplifier. The author assumes that the person using this circuit has a basic knowledge of FM radio principles. For a simple enhancement circuit, see page 104 of *Bench-Tested Circuits for Surveillance and Counter-surveillance Technicians.* This circuit can be part of a companion receiver to be used with the subcarrier converter on page 5 of *Bench-Tested Circuits.*



SCA decoder with general-purpose amplifier. This decoder setup can be used with high-quality spectrum analyzers by connecting it to the audio output (vertical out jack) of the analyzer.

OPERATE A BUG FROM A DC POWER ADAPTER

A long time ago, an investigative reporter asked me why it was so difficult to operate a "home-brew" covert transmitter from an AC-to-DC power adapter. The next day I sorted through my electronic junk boxes and came up with several DC power adapters that would handle the power requirements of the two "test" transmitters I had in my possession at that time.

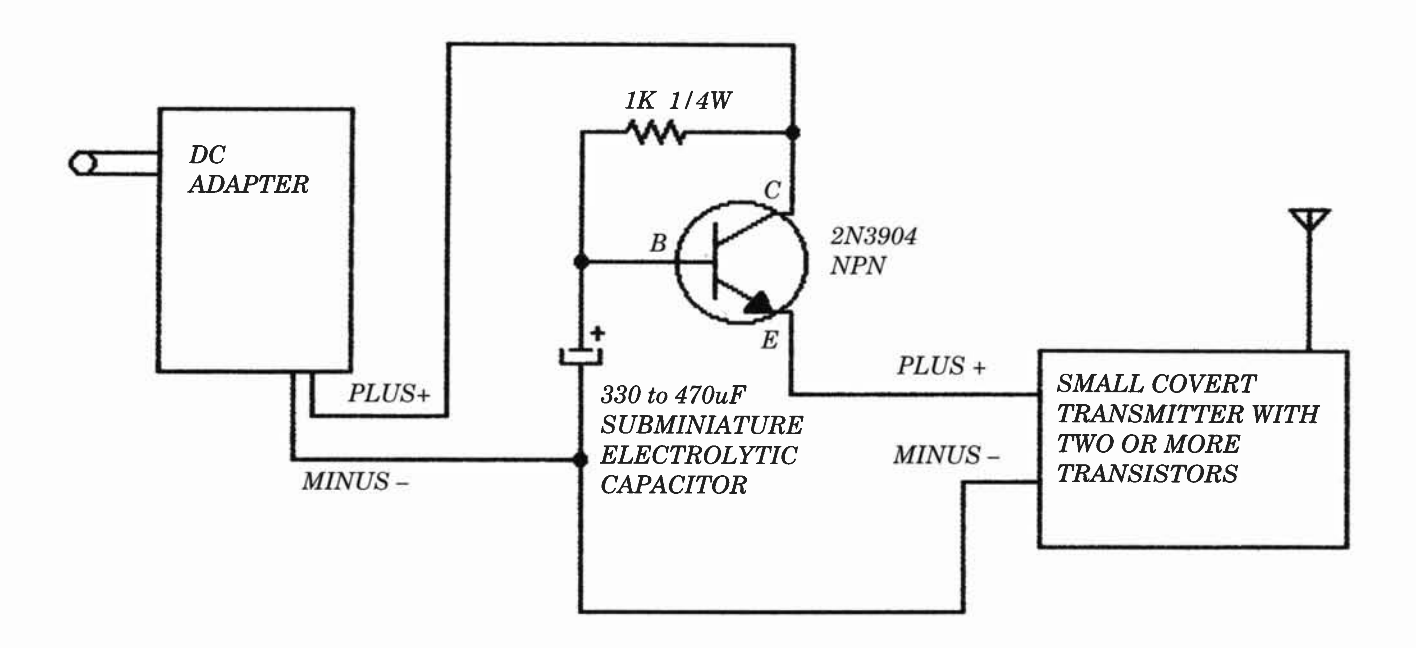
I tested each adapter with both test transmitters, and the results were horrible: very loud hum on a nearby FM radio tuned to the frequency, and frequency sweep to the point where one of the transmitters could have been used as a short-range radio frequency jammer! The test transmitter that acted like an RF jammer would sweep back and forth across the entire FM band on my spectrum analyzer!

I tried large value filter capacitors and some RF chokes; nothing seemed to work. Then I discovered this little "gem" of a circuit that eliminated the ripple and kept the transmitter dead on frequency!

Here is how it works.

The NPN transistor magnifies the value of the filter capacitor manyfold. In theory, the transistor's BETA x FILTER CAPACITOR IN uF = TOTAL CAPACITANCE IN uF. As you can see, the total capacitance of the filter capacitor could be increased with this circuit into the many thousands of uF.

IMPORTANT CAVEAT: Do not exceed the collector current rating of the transistor! One quick, cheap, and dirty way of determining the input power to a transmitter is to measure the total current used by the transmitter times the battery voltage (I x E = P).



NOTE: Most AC-to-DC adapters have far too much ripple (hum) to be used with covert transmitters. This circuit will allow you to use almost any 6- to 12-volt, 200- to 500-milliamp DC adapter.

CONSTRUCTION DETAILS: The circuit (transistor, resistor, and capacitor) can be mounted on the same board as the transmitter. Be sure to keep all leads from this circuit to the transmitter as short as possible. Perf board construction is more than adequate at VHF (very high frequencies) and lower. Make sure that the adapter will meet the power requirements of the transmitter.

OPERATE A BUG FROM A DC POWER ADAPTER

200-MEGOHM PHONE LINE INTERFACE

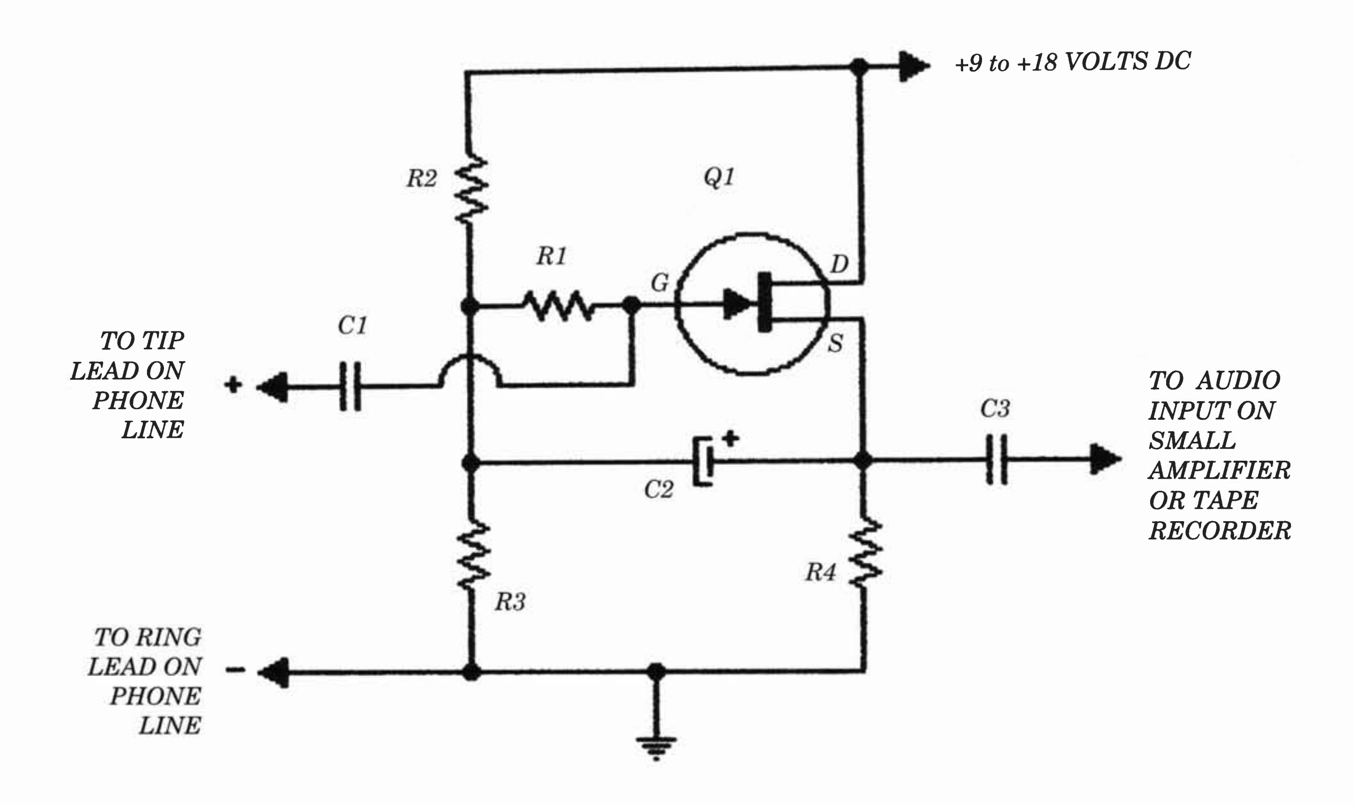
You will probably never meet a countermeasures person who is capable of finding this device, even using the best state-of-the-art electronic diagnostic equipment! The only way you could have any hope at all of finding it would be through a thorough physical sweep of the lines, i.e., a physical search of every linear foot of the phone line.

If the input leads on this device are kept less than 3 inches in length and are tied to an existing junction, a TDR tech—even with a fingerprint reading of the phone line—could not detect this device. If an operative is afraid a countermeasures team will use a leakage tester (as outlined in the first *Bench-Tested Circuits* book), all the operative has to do is replace C1 with a .001uF capacitor.

I conducted some experiments using the leakage tester, and I soon discovered that this circuit reads like a 50-foot piece of phone cable open at both ends when C1 is changed to .001uF. Audio quality was still good when C1 was replaced with a .001uF capacitor. Satisfactory performance was realized with the use of a 9-volt battery. Current drain was only 600 microamps!

CONCLUSION: If the operative keeps the leads short and changes C1 to .001uF, this circuit will be invisible (electrically speaking) to TDR sweeps and leakage testers with little or no audio degradation.

THIS CIRCUIT SHOULD MAKE ANY PHONE LINE BRIDGE JOB INVISIBLE TO TDR SWEEPS!



NOTE: C2 increases the value of R1 20-fold due to "bootstrapping."

PARTS LIST FOR THE JFET SOURCE FOLLOWER:

Q1 – MPF102 or NTE451 or NTE 312 N-channel field effect transistor
R1 – 10 megohm 1/4-watt resistor (Do not exceed 10 megohm.)
R2 – 270K ohm 1/4-watt resistor
R3 – 150K ohm 1/4-watt resistor
R4 – 6,500 ohm 1/4-watt resistor
C1 – .1uF capacitor
C2 – 1uF electrolytic capacitor
C3 – .1uF capacitor

NOTE: (Q1) – G=Gate, D=Drain, S=Source
Two 9-volt batteries could be hooked in series to obtain 18 volts.

VERY IMPORTANT NOTE: In order to avoid time domain reflectometer (TDR) sweeps, leads from circuit to phone line should be less than 3 inches in length and should be connected to an existing junction.

200-MEGOHM PHONE LINE INTERFACE

80-MEGOHM AUTOMATIC TAPE STARTER

Here is a reliable, goof-proof automatic tape starter with a very high input impedance. If the leads that connect to the phone line are kept very short (less than 3 inches), this circuit will be invisible to the phone company and, more than likely, to the best countermeasures teams in the country. However, this circuit has one definite vulnerability: it can be detected by my "Leakage Checker" (see the first *Bench-Tested Circuits* book).

Soon after I bread-boarded this circuit, I made the following observations after connecting the "Leakage Checker" to the input of the circuit:

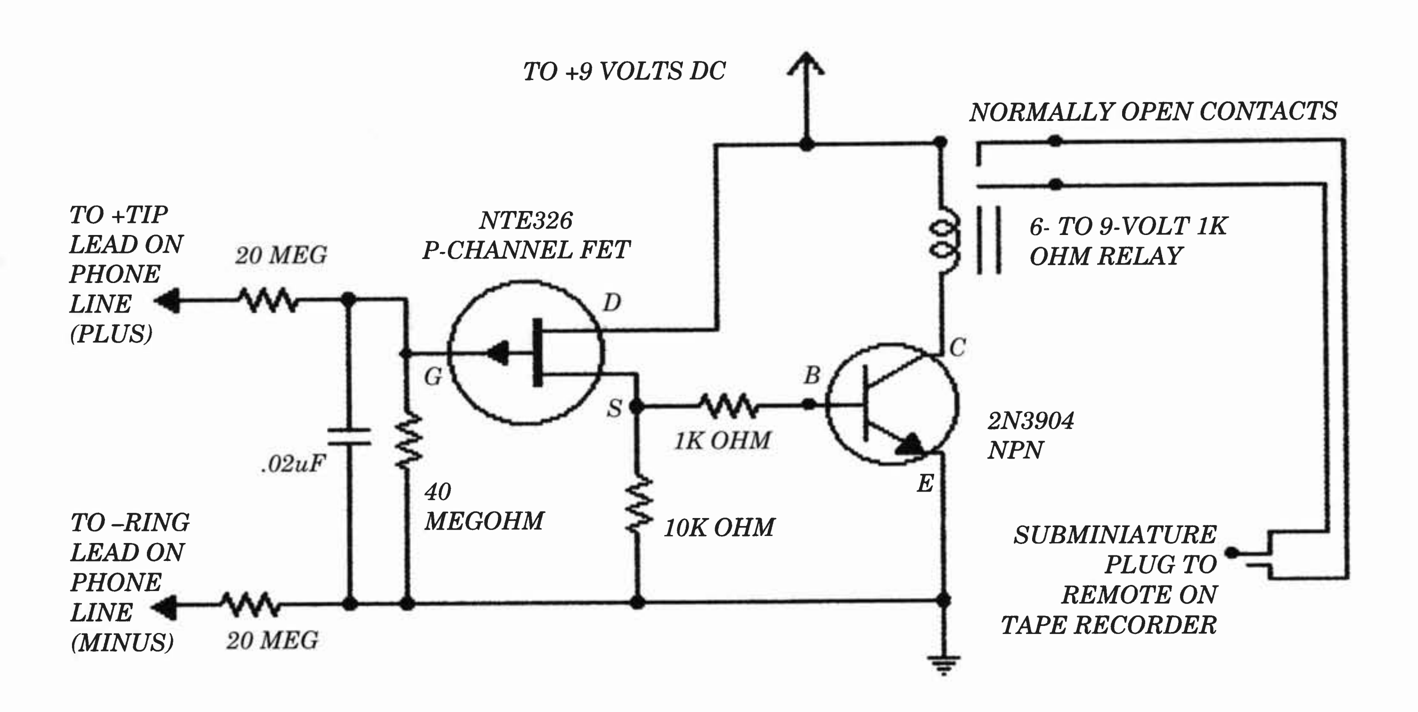
1) The needle of the Leakage Checker gave a reading similar to one that you would obtain if you had connected it to a 500-foot piece of phone cable that was open at both ends.
2) Because the circuit is resistive, *the needle did not settle back down to zero.* It stayed at the same reading you would normally get when you would measure 400 to 500 feet of phone cable that was open at both ends.

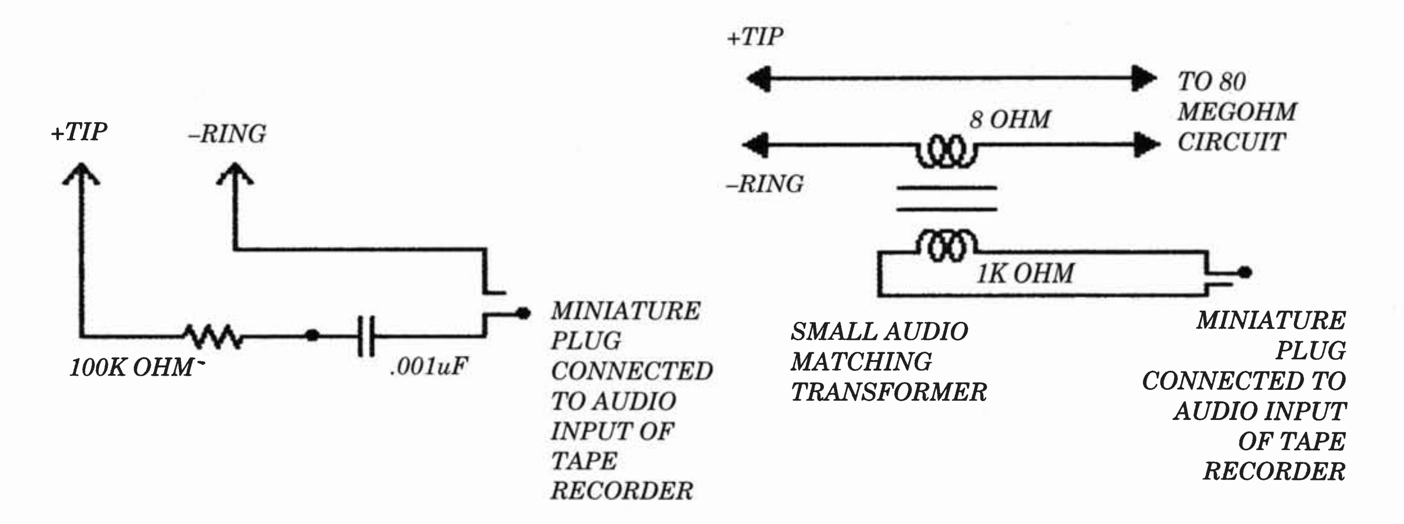
SOME VERY IMPORTANT OBSERVATIONS

When you measure a capacitor input device with a leakage checker, the needle will deflect upward across the scale and then settle back down to zero. If you measure a device that is resistor coupled, the leakage checker will deflect upward across the scale and stay at a high reading.

THE TELEPHONE COMPANY IS NOT GOING TO LET YOU EXAMINE ITS JUNCTION BOXES OR DISCONNECT LARGE PORTIONS OF ITS PHONE LINES!

PLEASE NOTE: if you want the basic theory on this circuit's operation, refer to the "Phone Line Usage and Cut Monitor" circuit in Section 1 of this book.





IMPORTANT NOTE: All leads from circuit to phone line must be less than 3 inches and connected to existing phone line junction points!

NOTE: All resistors are 1/4 watt.

NOTE: Leads connected to output side of the circuit may be any convenient length.

80-MEGOHM AUTOMATIC TAPE STARTER

TELEPHONE RING DETECTOR/TRIGGER

The following circuit allows you to control equipment or bugging devices from anywhere in the world. It is best used on a second, unlisted phone line and, in some cases, perhaps that second line should be billed to another address. Let's take a closer look:

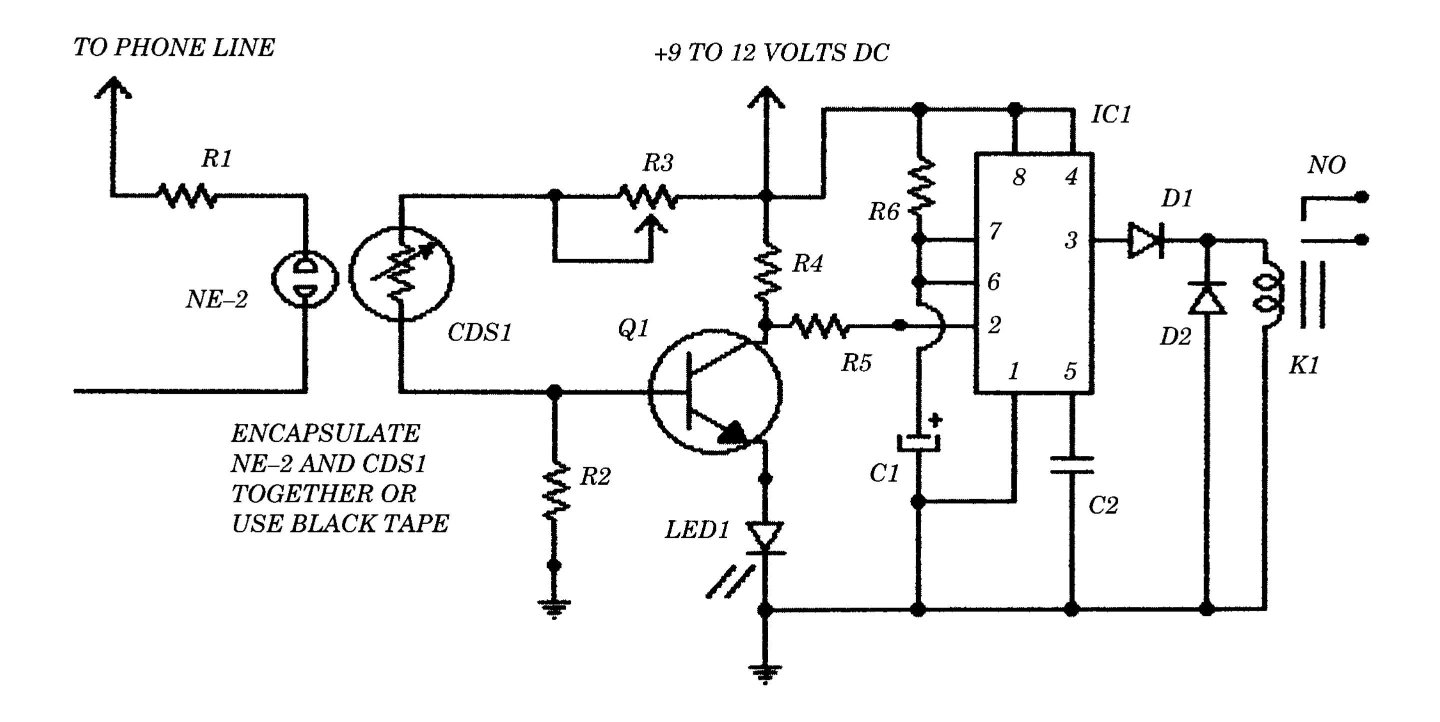
When the AC ring voltage activates the NE–2 (neon light), the CDS1 (photo resistor) resistance drops dramatically, thereby turning on transistor Q1 in cadence with the AC ring signal. The instant that transistor Q1 turns on, pin 2 (IC1) receives a negative pulse, thus giving us a positive pulse at pin 3 (IC1) for a time period determined by R6 and C1. With this positive pulse at pin 3 (IC1) the relay will be energized for a time duration, again, determined by R6 and C1 (Time = R6 x C1).

R3 is the sensitivity control. This allows for variations or lack of uniformity in the manufacture of the CDS1 or the NE-2 and also the technician's construction practices. Generally speaking, the setting of R3 can be done in the lab.

If this circuit is to be used for bugging, then you would delete K1 (relay) and D1 and D2 (diodes) and use the high-voltage NPN transistor as shown in the options schematic. The NPN transistor will answer the phone line (electronically) for a time period determined by R6 x C1 = T. At this point you would need a tone decoder circuit, a relay, and a small audio amp with microphone. The tone decoder would be attached to the unlisted phone line and, when activated from the listening end, would energize the relay, which would turn on a hidden audio amp with microphone. The tone decoder could also be made to trigger pin 2 of IC1 to keep reactivating the time delay.

If you need some tips and techniques on using tone decoders, encoders, and covert audio amps and phone line connection methods, please refer to *Bench-Tested Circuits for Surveillance and Counter-surveillance Technicians*. It should give you some good springboards (ideas).

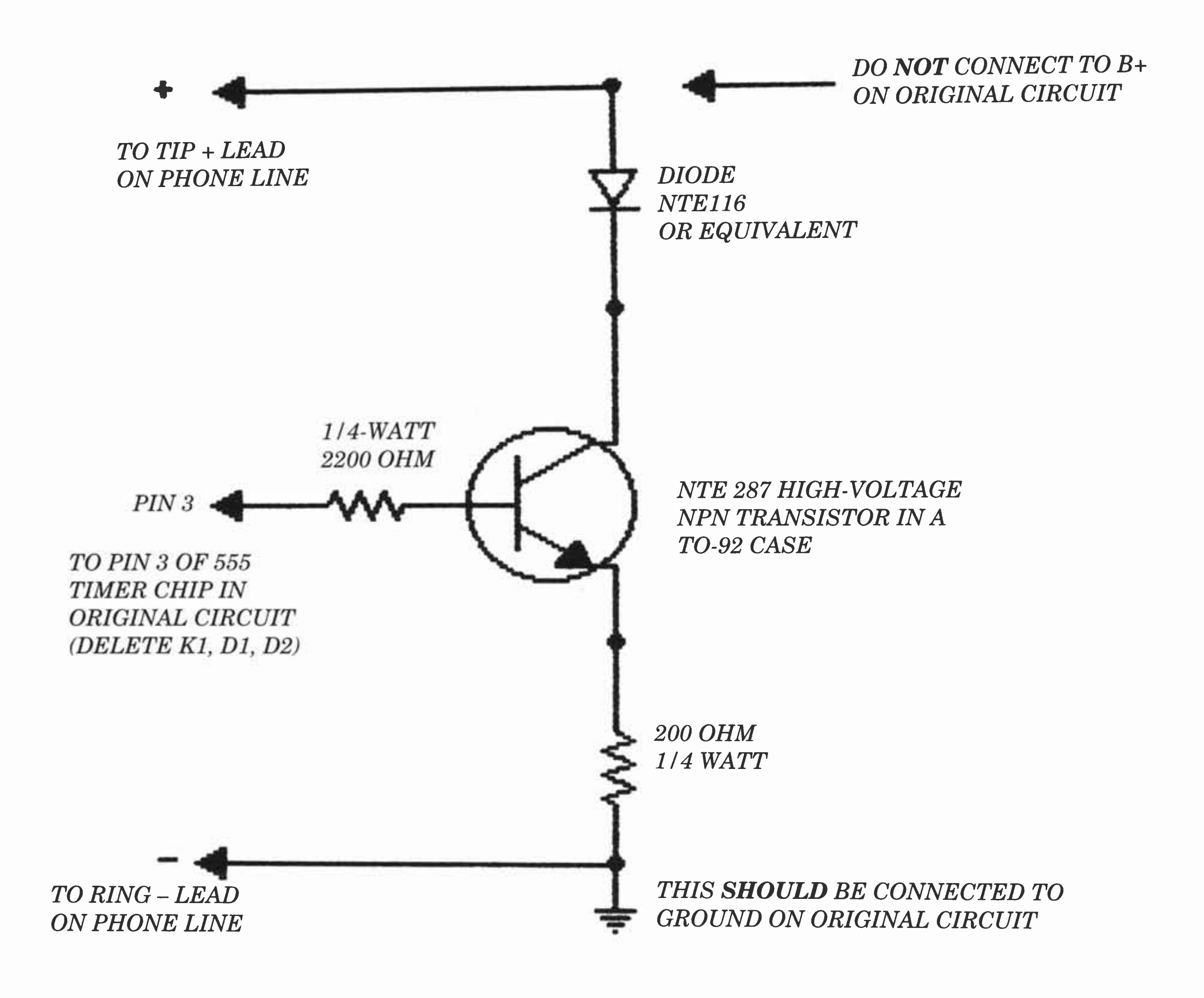
For you modern types who want a more updated ring detector circuit, please look at the bottom schematic on the options for telephone ring detector/trigger page. Take a good look at what components it replaces. We now have 5 versus 9 components. When triggered, pin 5 outputs a negative pulse in cadence with the AC ring voltage (signal).



PARTS LIST:

NE-2 – neon light
CDS1 – photo resistor
Q1 – 2N3904 or 2N2222 NPN transistor
IC1 – 555 timer IC
LED1 – light-emitting diode
D1, D2 – 1N914 silicon diodes (relay coil spike prevention)
R1 – 220K ohm 1/4-watt resistor
R2 – 1,000 ohm 1/4-watt resistor
R3 – 10K ohm potentiometer (sensitivity control)
R4 – 330 ohm 1/4-watt resistor
R5 – 2,700 ohm 1/4-watt resistor
R6 – 1 megohm 1/4-watt resistor (sets time delay)
C1 – 100uF electrolytic capacitor (sets time delay)
C2 – .01uF capacitor
K1 – 500- to 1,000-ohm, 6- to 9-volt relay

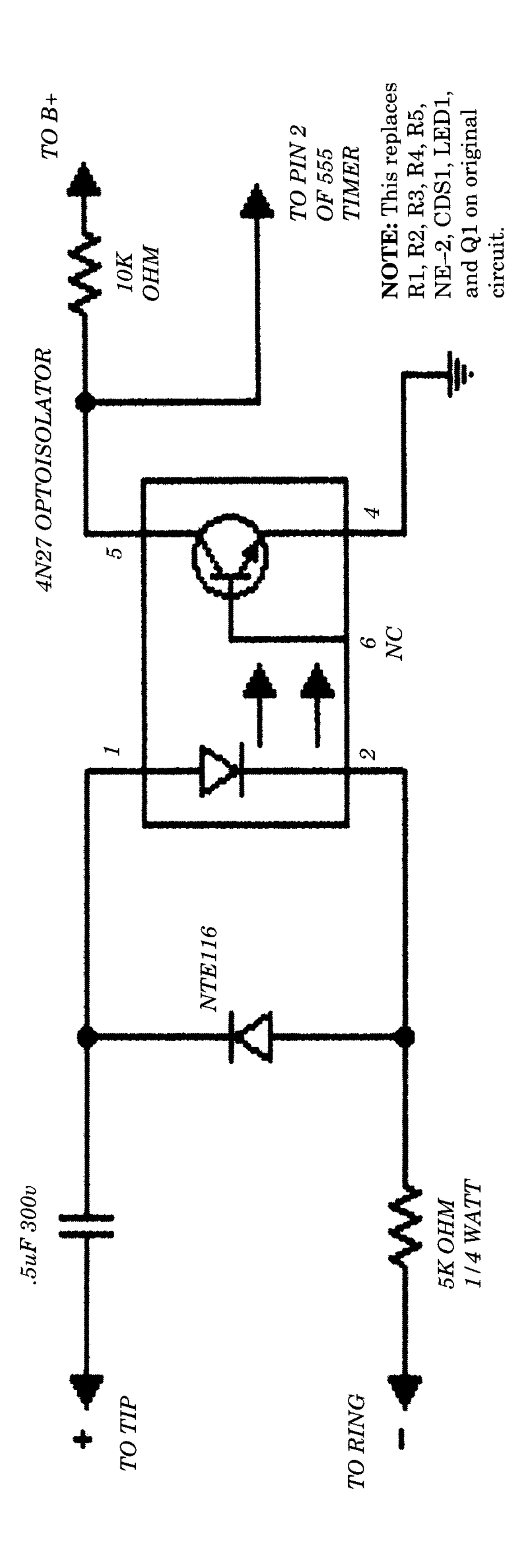
TELEPHONE RING DETECTOR/TRIGGER



***NOTE:** Refer to original "Telephone Ring Detector/Trigger" schematic.*

IMPORTANT OPERATIONAL NOTES: This optional circuit replaces relay K1 in the original circuit. It answers the phone for a time period determined by R6 and C1 in the original circuit. This circuit effectively takes the phone off the hook, temporarily.

OPTIONS FOR TELEPHONE RING DETECTOR/TRIGGER


TO B+
10K
OHM
TO PIN 2
OF 555
TIMER
NOTE: This replaces R1, R2, R3, R4, R5, NE–2, CDS1, LED1, and Q1 on original circuit.
4N27 OPTOISOLATOR
5
4
6
NC
1
2
NTE116
.5uF 300v
5K OHM
1/4 WATT
+
TO TIP
TO RING
-

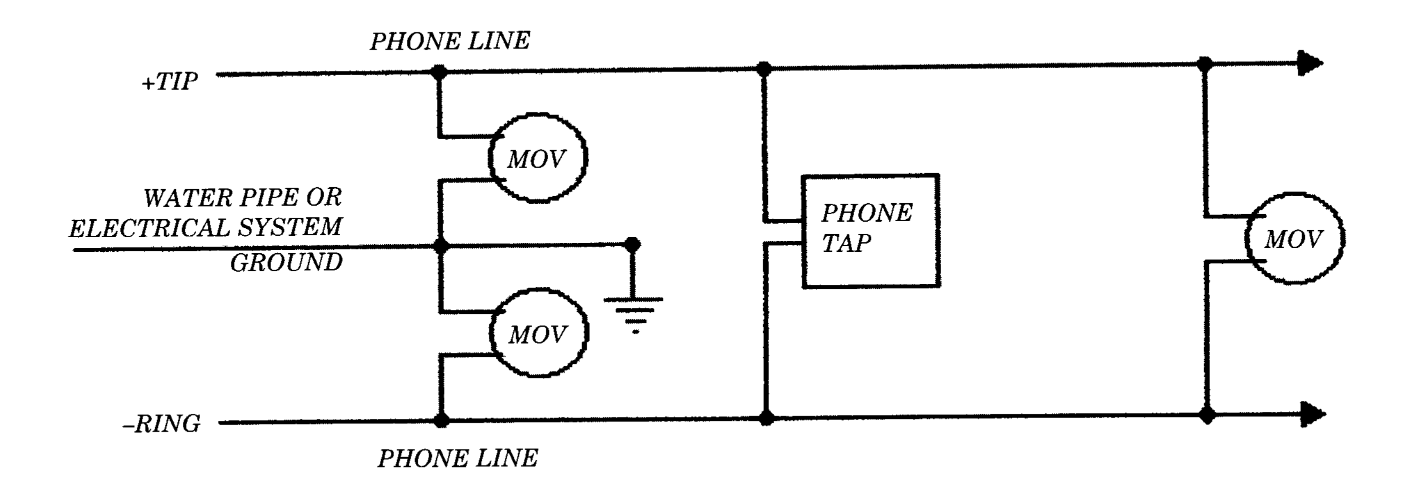

HERE IS ANTOHER RING DETECTOR CIRCUIT

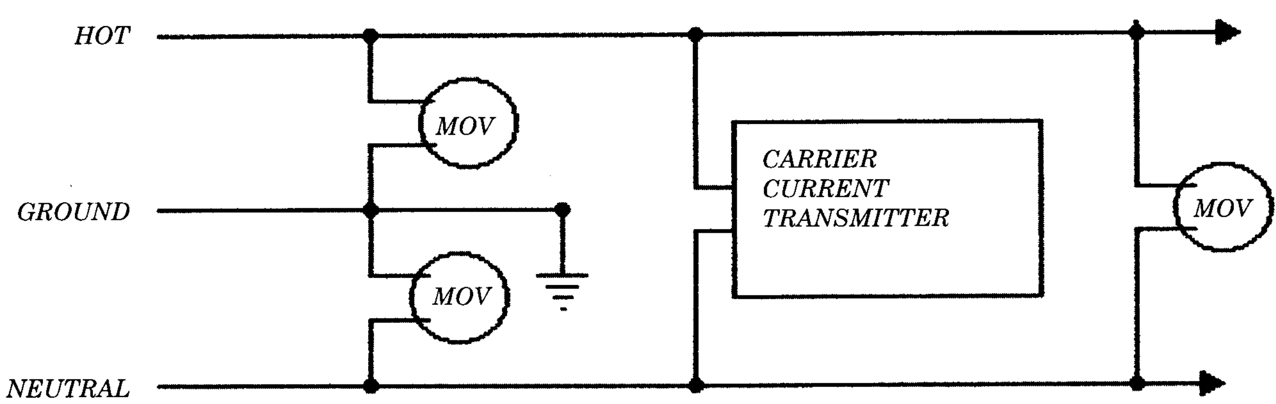
HIGH-VOLTAGE SPIKE PREVENTION

It would be a good idea to examine my "Incendiary Destruction of Inaccessible Taps and Line-Connected Bugs" project in Section 1 of this book.

The following protection scheme is not foolproof. If the countermeasures technician uses a high-voltage (current limited) neon sign transformer repeatedly, the metal oxide varistors (MOVs) are not going to survive! However, this protection scheme should offer good protection from many of the worthless high-voltage "bug and tap burning" device schematics I have seen over the years.

This protection scheme can be used with phone lines and with AC power lines. Always use the heavy-duty type MOVs. For increased protection you could put extra MOVs in parallel with each other. The redundancy of placing MOVs in parallel is a good idea because they do tend to fail over time under normal use.





MOV: HEAVY-DUTY METAL OXIDE VARISTOR, AVAILABLE AT MOST ELECTRONIC SUPPLY COMPANIES AND RADIO SHACK.

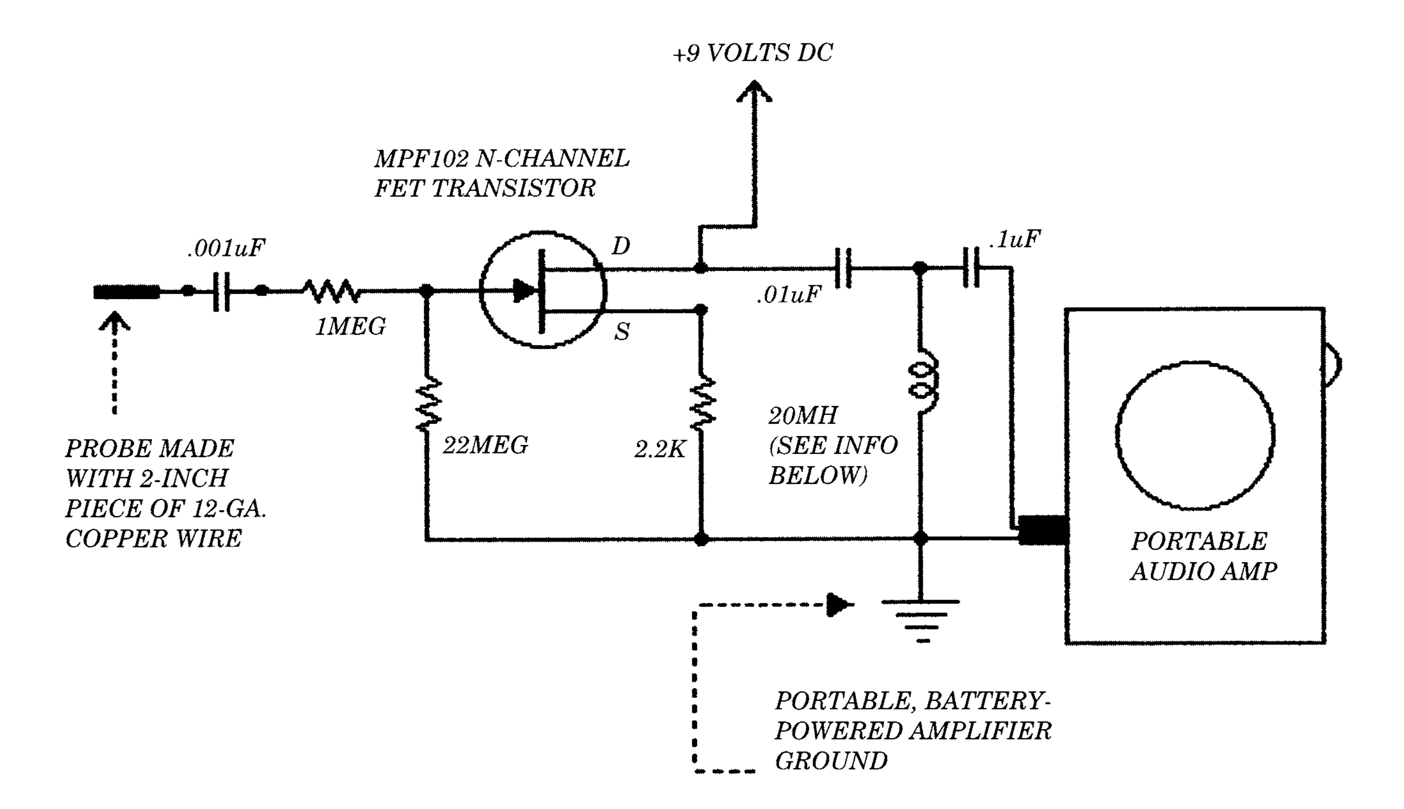
APPLICATION NOTE: This should give some protection to phone-line- and electrical-line-connected eavesdropping devices. When a very high-voltage spike occurs, the MOV will "clamp" (lower its resistance) within a few microseconds.

HIGH-VOLTAGE SPIKE PREVENTION
(IS SOMEONE TRYING TO BURN YOUR DEVICE OFF THE LINE?)

INDUCTIVE PROBE FOR PHONE LINES

Here is a telephone tap that the best countermeasures person in the world *cannot* detect! The inductive probe tip only touches one phone line terminal (or wire). There is no completed circuit; the probe only receives the audio or data by inductive coupling. This is analogous to a portable radio receiving a broadcast station. Nothing is drained or taken away (electronically speaking) from the phone line with this circuit.

This circuit works as well as or better than some of the inductive probes I used during my one-year stint in the telecommunications industry. You may want to experiment with different component values and packaging arrangements to suit your needs. Speaking of packaging, you might try installing this circuit in a small shielded box and then placing it inside a plastic project box. You could use a feed-through capacitor from the metal box to the probe. The audio quality could be enhanced by a really tight band pass filter connected to the input of an amplifier.



APPLICATION NOTES: 20-millihenry choke should have 40 to 60 ohms DC resistance. You can try different values to suit your needs. The probe could be a 2-foot piece of wire with an alligator clip. Keep all leads on circuit board short and use a short piece of shielded cable from amp to circuit board. The author used a small shirt-pocket-sized portable amplifier from Radio Shack.

IMPORTANT: Don't let the simplicity of this circuit fool you. This circuit can be very touchy! Some phone lines will induce more noise than others, and the noise levels can be quite unbearable!

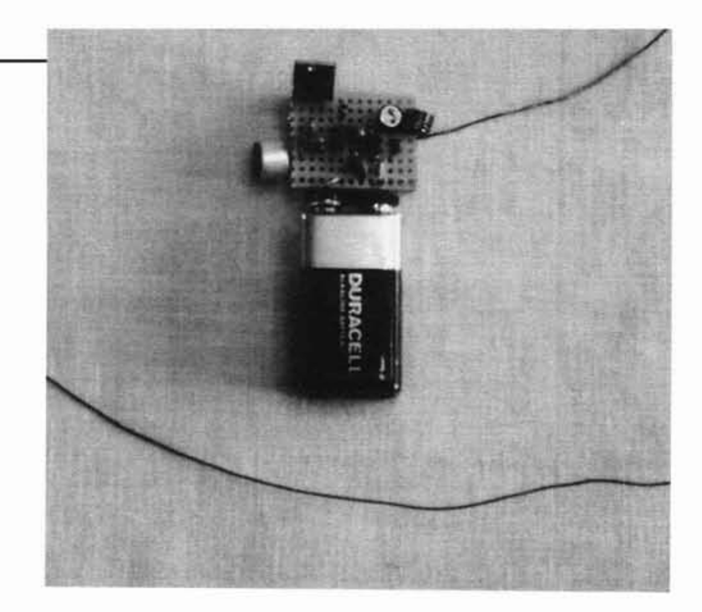
INDUCTIVE PROBE FOR PHONE LINES

A SIMPLE TECHNIQUE FOR IMPROVING THE STABILITY OF A COVERT TRANSMITTER

The following transmitter modification will not give you crystal control; however, it will give you a frequency stability that one rarely experiences while experimenting with two-transistor "home brew" transmitters.

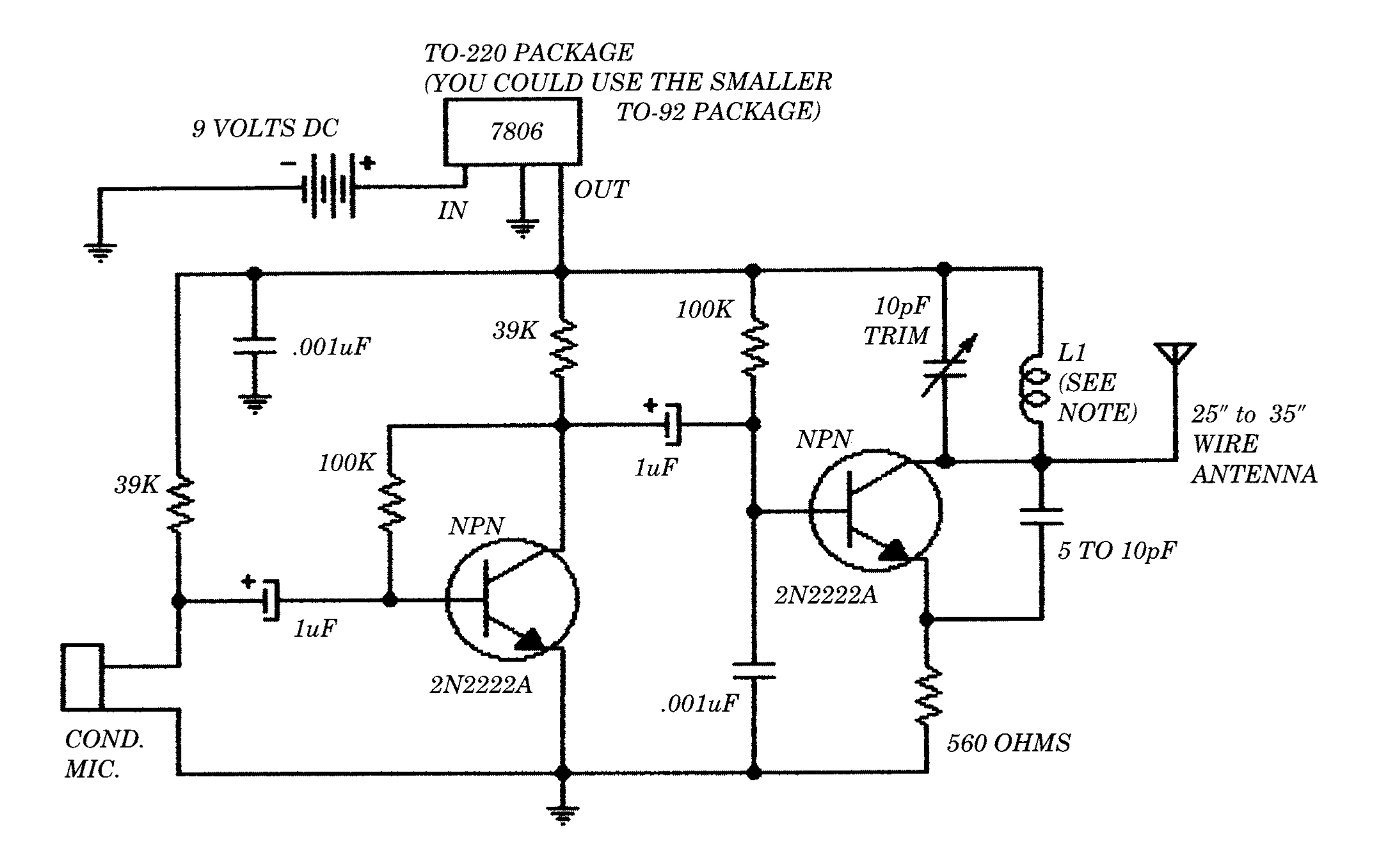
The heart of this modification is the 7806 voltage regulator. This regulator keeps the voltage constant. When you work with small, unstable oscillators such as your basic covert transmitters, they tend to drift as the battery drains. Obviously, if we could keep the voltage at a constant level, the transmitter would stay dead on frequency.

When this circuit was viewed on a spectrum analyzer, the harmonics were reduced and oscillator damping was almost eliminated. I could get within a fraction of an inch from the oscillator without shutting it down, due to body capacitance. Before the regulator circuit was installed, the oscillator would shut down if I got within three inches of the transmitter. Oscillator drift due to body capacitance was greatly reduced *but it still did not approach the stability of crystal control.*



Not quite crystal control, but very close. Generic two-transistor transmitter with voltage regulator shown at upper left-hand corner of the circuit board. The author used a TO-220 package. In most cases the much smaller TO-92 package can be used. If you decide to use the TO-92 voltage regulator IC, be sure that it will meet the milliamp requirements of the transmitter.

THIS IS THE SECRET: THE 7806 VOLTAGE REGULATOR GREATLY INCREASES THE STABILITY OF THE TRANSMITTER.



NOTE: L1 – 6 turns, 22-gauge, enamel-covered wire, 1/4-inch diameter. The two 2N2222A transistors should be matched, i.e., same lot and batch. The two 1uF caps should be miniature electrolytics. The resistors should be 1/8 watt.

APPLICATION NOTE: Author's prototype had an 8-milliamp draw. Five milliamps were drawn by the voltage regulator, and 3 milliamps were drawn by the transmitter. The transmitter was tuned to 79 MHz (CH5 TV), which is not in use in my area. Range was 200 feet in a suburban area. A weak second harmonic was noticed at 158 MHz. Audio sensitivity and sound quality were very good.

A SIMPLE TECHNIQUE FOR IMPROVING THE STABILITY OF A COVERT TRANSMITTER

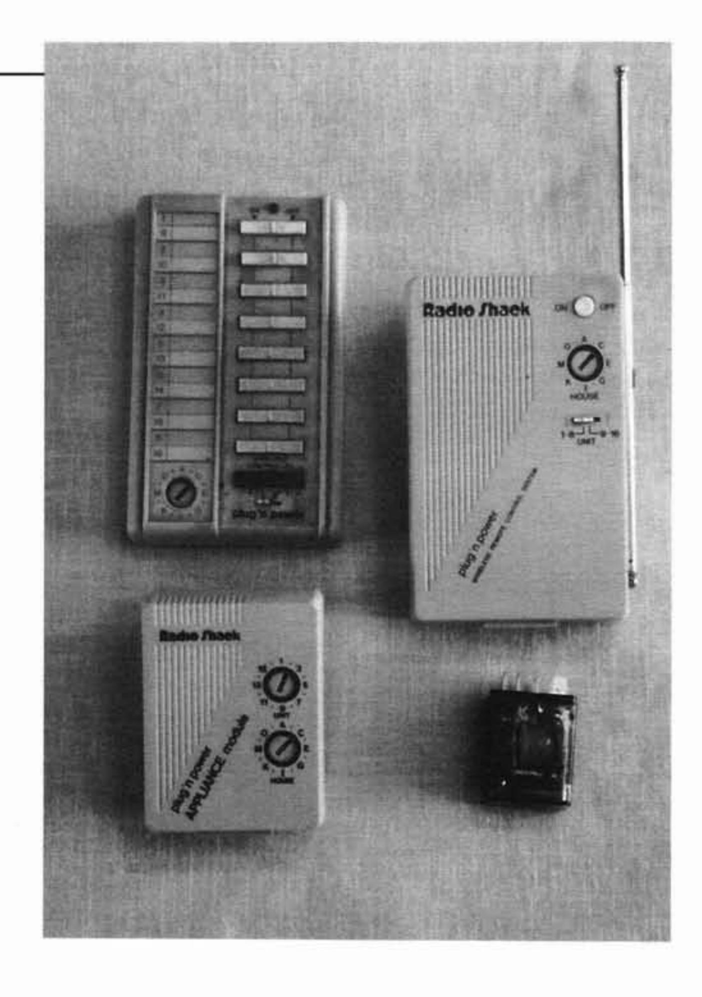
SIMPLE, RELIABLE RADIO CONTROL FOR BUGS

Back in 1990 a private investigator invited me to her office to give a talk on surveillance and countersurveillance to a group of local private investigators. Some of these "seasoned" PIs were skeptical when they heard that I was going to demonstrate a bug and a tap that the best countermeasures team in the world could not find by electronic means. Their collective eyebrows were really raised when they were told that the entire system cost me less $100 retail. Let's take a look at the system.

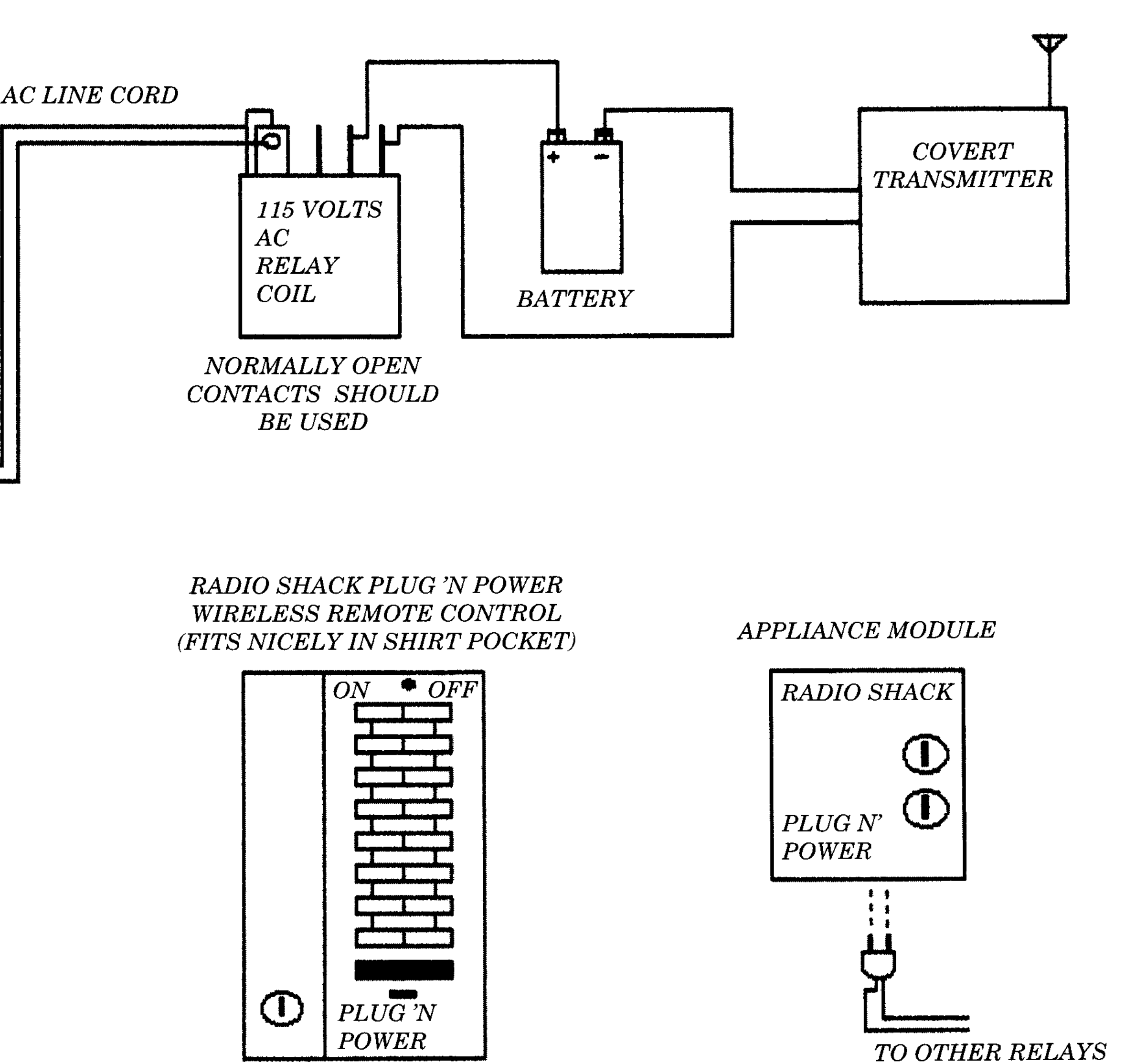
I bought a Plug 'n Power RF remote, a Master Control Module and an Appliance Module from Radio Shack (my favorite store). The remote had a 300-foot range (more than adequate). I also bought a 115 volts AC coil relay from Mr. Tandy. With the addition of a battery, a home-brew bug, a home-brew phone tap, an AC line cord, and a 2-foot patch cord with alligator clips at both ends, I was now ready for my demonstration.

When I explained the system to these PIs, they were absolutely flabbergasted at its simplicity, reliability, low cost, and ability to be made invisible at the touch of a button. One of them asked me about Non-Linear Junction detection (in a rather snide way) and I shot back at him with the following: "Ever heard of aluminum foil shielding?" He was obviously trying to trip me up, but he acquiesced when I foiled him with my quip about aluminum foil.

WITH A LITTLE WORK THIS INEXPENSIVE SYSTEM COULD BE MADE TOTALLY INVISIBLE TO MOST ELECTRONIC DETECTION METHODS!



With this system you can have reliable radio-controlled "turn-on, turn-off" capability for covert transmitters. Starting from the upper left and working clockwise: remote control, master control module, 115 Volts AC (coil) relay, and slave module for an additional device.



APPLICATION NOTE: You can have up to 16 modules with 16 different codes. You could turn on and turn off up to 16 covert devices. Use a patch cord with alligator clips to attach modules to 115 Volts AC wiring.

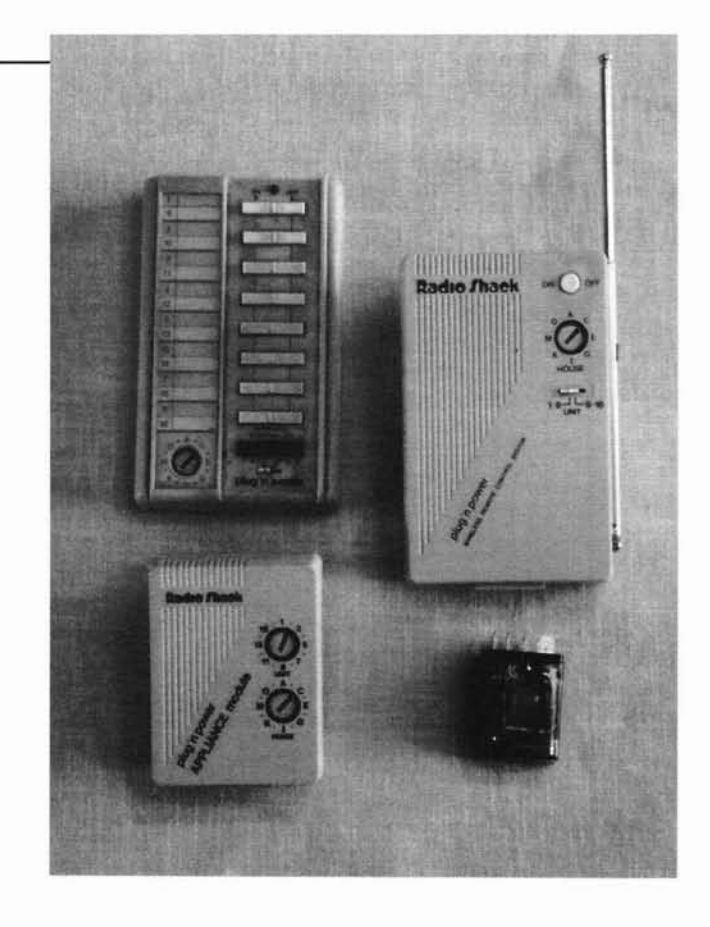
SIMPLE, RELIABLE RADIO CONTROL FOR BUGS

A SIMPLE WAY TO MAKE A TELEPHONE TAP INVISIBLE AT THE PUSH OF A BUTTON

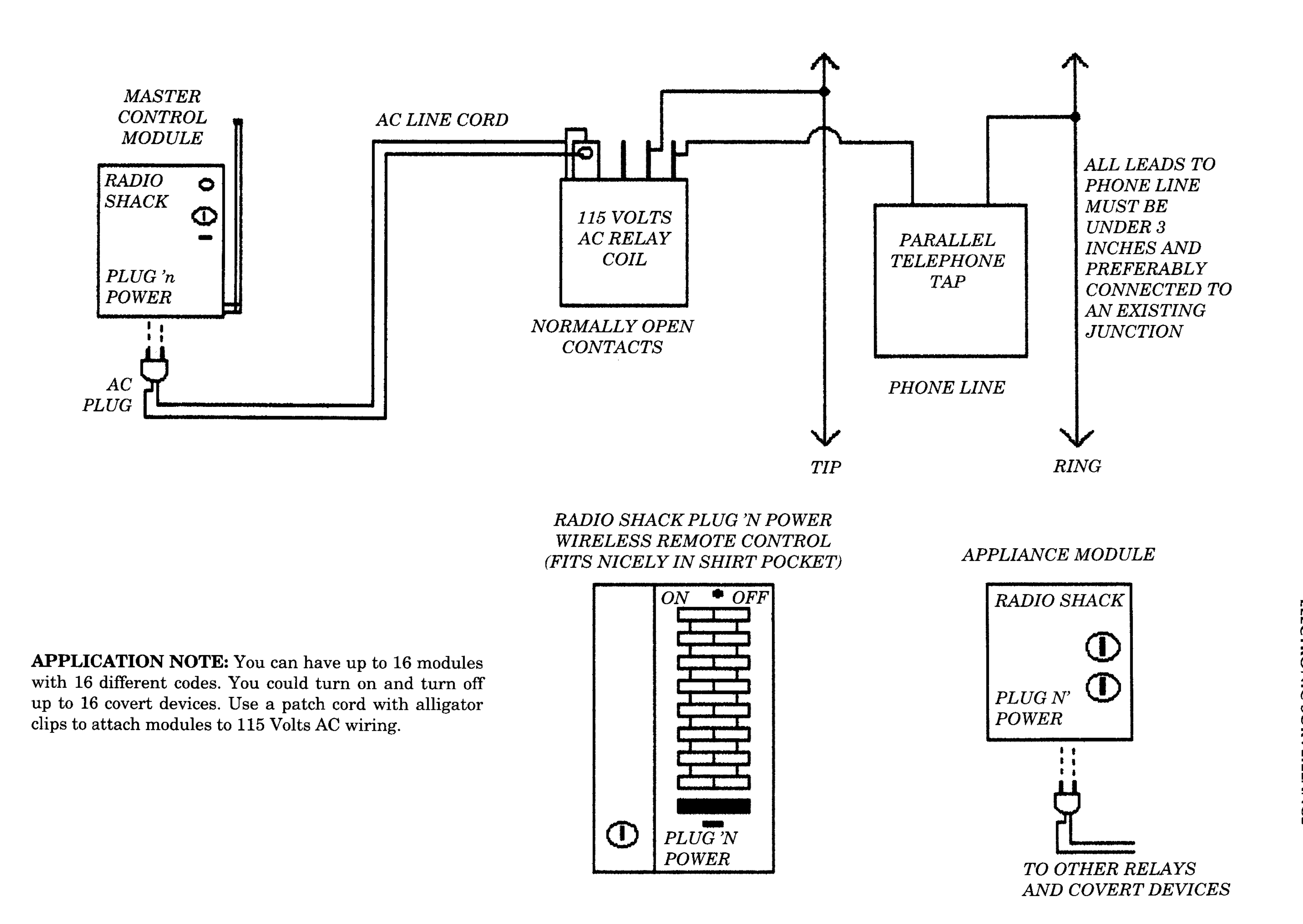
The background and story on this one is actually a continuation of the "Simple, Reliable Radio Control for Bugs" that precedes it.

This was one of my first attempts at making a telephone tap invisible to electronic detection equipment. The only problem with this system is that you have to be within line of sight or get tipped off somehow that a countermeasures team is on the way. Fortunately for the telephone tappers, almost all clients tip their hand by using a phone to call up the local countermeasures jockey (or rain dancer)! Let's take a closer look at the system.

If the leads are kept at less than 3 inches and the tap is disconnected by the relay, a leakage checker and a TDR are not going to detect anything, period! This same concept would work quite well for a series-connected tap by using the relay to short out the input leads to it. This system could be hidden in false ceilings, basements, attics, phone closets, and wherever phone and electric lines run. You will need lots of luck finding this one!

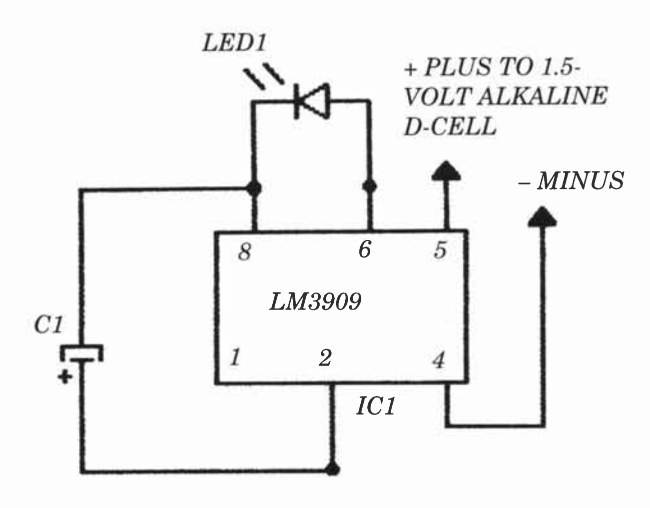


Telephone tap cloaking device. With the following system you can make a telephone wire tap invisible with "turn-on/turn-off" capability. Starting from the upper left and working clockwise: remote control, master control module, 115 Volts AC (coil) relay, and slave module for an additional device.



A SIMPLE WAY TO MAKE A TELEPHONE TAP INVISIBLE AT THE PUSH OF A BUTTON

VERY-LOW-POWER *INFRARED* FIREFLY TAGGER
(DON'T OVERLOOK THIS ONE)



PARTS LIST:

IC1 – LM3909 flasher integrated circuit
LED1 -infrared LED
C1 – 330uF electrolytic capacitor (determines flash rate)

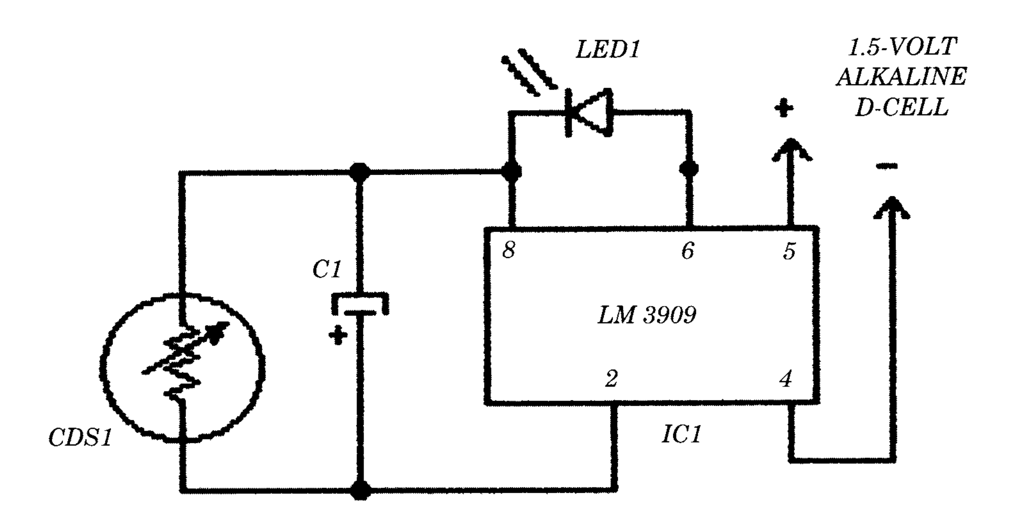
APPLICATIONS NOTE: This flasher can only be seen with infrared night vision equipment. *It will last one year or more* with a 1.5-volt alkaline D-cell. It is not as bright as my high-powered flasher circuits as outlined in the first Bench-Tested Circuits. This circuit is great for tagging stashes, targets, rendezvous, and caches.

VERY IMPORTANT: Due to the low power of this device, you should have a general idea as to its approximate location, i.e., within 100 feet (maximum) for an urban area with many street lights and perhaps 300 feet in a wilderness area, depending on the direction of the approach, ground cover, and terrain. Flash rate is very slow, thereby *reducing power consumption and making it harder to spot.*

This is a surplus night vision scope that worked quite well with the "Infrared Firefly Tagger." Be careful not to point this or any night vision scope directly at a light source, e.g., street lights, porch lights, lamps, and so on. Do not use night vision equipment during daylight! Surplus night vision equipment will tend to degrade or be destroyed if the above-mentioned advice is not adhered to.



DARK-ACTIVATED LOW-POWER INFRARED FIREFLY TAGGER



PARTS LIST:

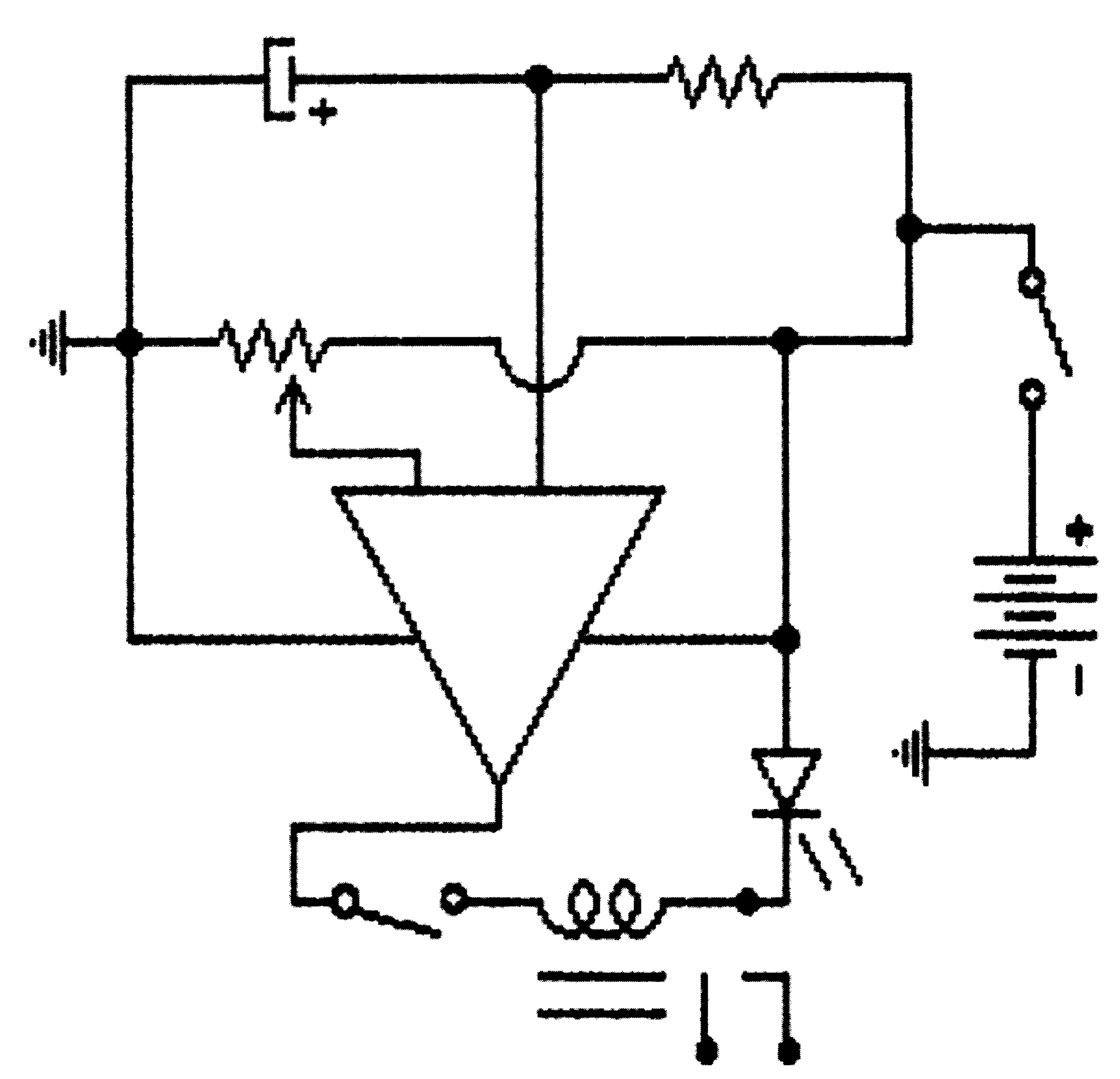
IC1 - LM3909 flasher
LED1 – infrared LED
C1 – 470uF electrolytic capacitor
CDS1 – photo resistor (I used a 500-ohm-in-light, 10-megohm-in-darkness photo resistor.)

APPLICATIONS NOTE: This flasher can only be seen with infrared night vision equipment. The photo resistor activates the flasher at night. This circuit should last one year or more with a 1.5-volt alkaline D-cell.

IMPORTANT: Be sure to read the applications note and important information on the "Very Low Power Infrared Firefly Tagger" (p. 48). *The photo resistor reduced power consumption by almost 50 percent in my prototype.*

SECTION III

MISCELLANEOUS



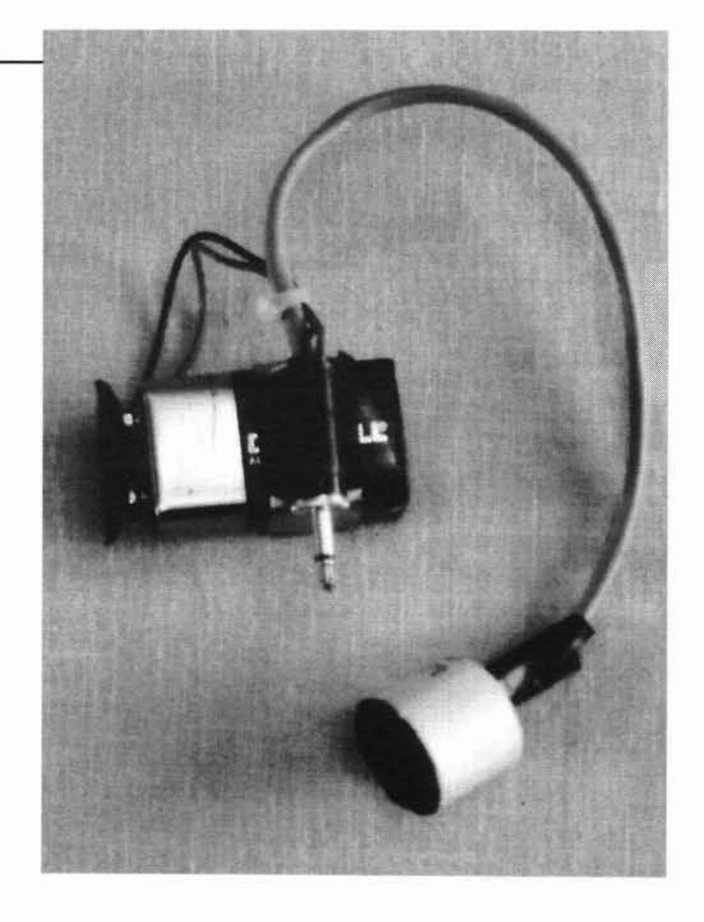
(BUGGER'S LITTLE HELPERS)

HOW TO MODULATE A LASER BEAM

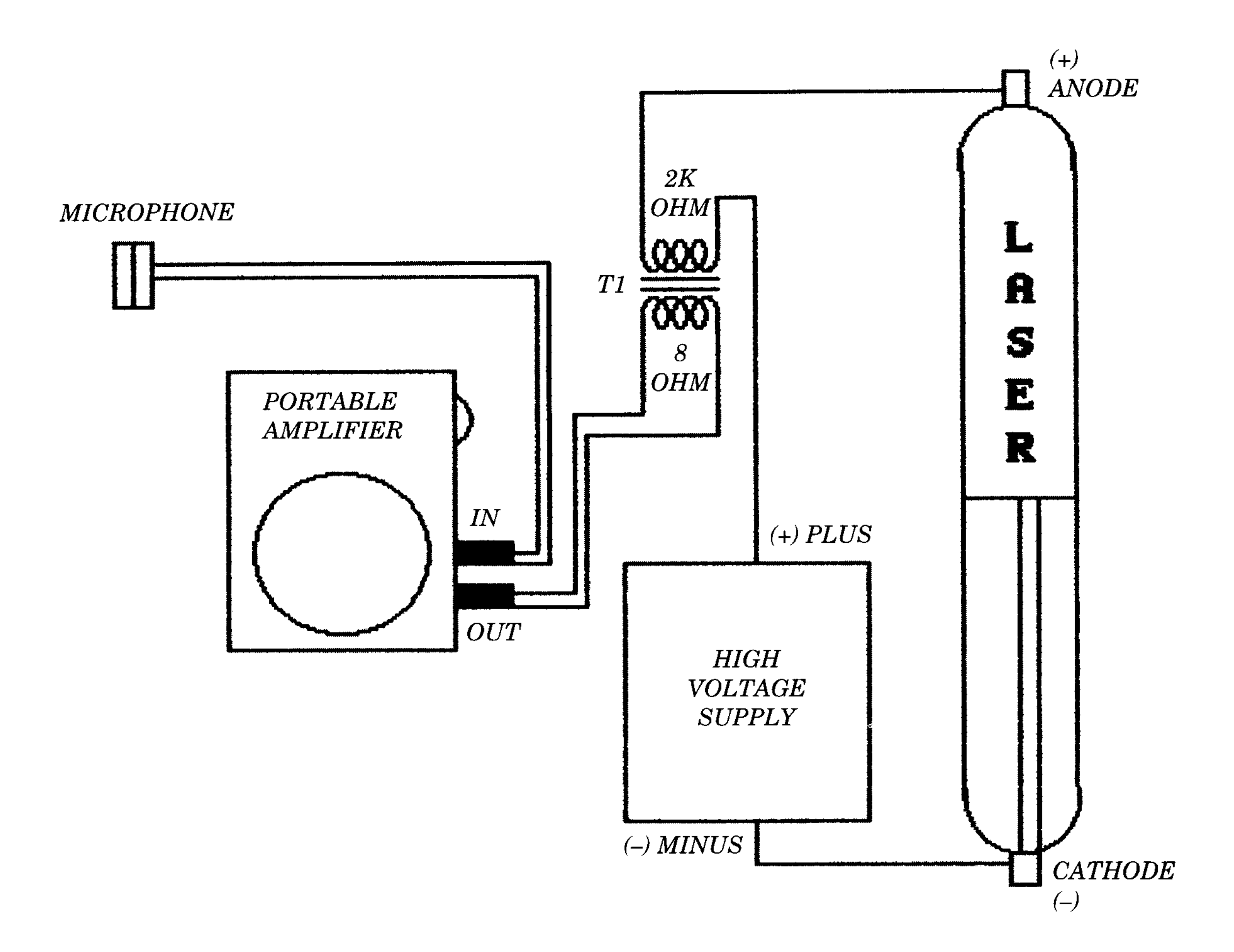
The following modulation scheme can be used to modulate a Helium-Neon Laser. The following circuit offers some interesting possibilities for line-of-sight communications links. This circuit can be used in conjunction with my "Easy-to-Build Lightwave Receiver" (featured in *Bench-Tested Circuits*). That lightwave receiver can be greatly improved by placing a piece of color film negative over the end of the 3/4-inch PVC pipe section. I would also place a fair amount of distance between the laser and the lightwave receiver when testing this system. Let us examine the circuit.

A dynamic microphone is used with a small portable amplifier and a small audio matching transformer (8 ohm x 2K ohm) to modulate the high voltage supply. The 2K ohm side of the transformer is placed in series with the anode (+) of the Helium-Neon Laser tube and the plus side of the high voltage supply. The 8-ohm side of the transformer gives us a good impedance match to the output of the amplifier.

Application: You could set up a temporary covert communications system with the setup listed above. Due to the fact that the laser is so highly directional, the possibility is very remote that anybody would intercept the communications, especially if the communications were kept very short in duration.



This can be used on the receiving end (with a small battery-powered amplifier). See the "Easy-to-Build Lightwave Receiver" in Bench-Tested Circuits for Surveillance and Countersurveillance Technicians. The above IR photo transistor assembly should be covered with an exposed color film negative in order to reduce interference from ambient light sources.



WARNING: LASERS HAVE TWO POWER SUPPLIES—ONE LOW-VOLTAGE SUPPLY AND ONE DANGEROUSLY HIGH-VOLTAGE SUPPLY. DO NOT LOOK DIRECTLY AT A LASER BEAM! THIS IS NOT A TOY.

PARTS LIST:

Most any generic, helium-neon (or similar) laser
Portable Radio Shack amplifier
Small dynamic microphone
Patch cords
Miniature plugs
T1 – small audio matching transformer,
8 ohm to 2K ohm

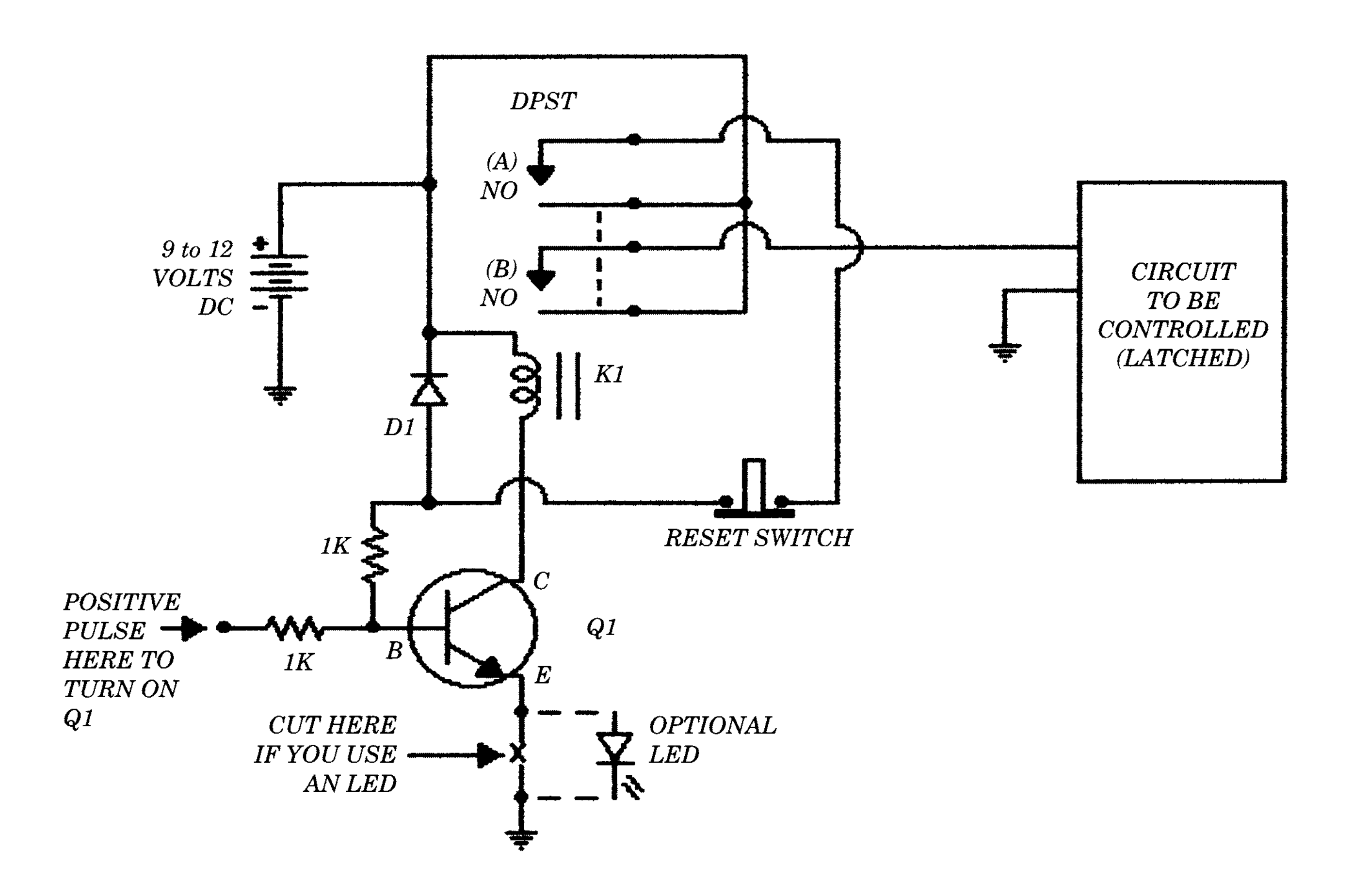
HOW TO MODULATE A LASER BEAM

HOW TO TURN A DPST RELAY INTO AN SCR

(YOU WON'T NEED A SENSITIVE-GATE SCR WITH THIS CIRCUIT)

Throughout this book and *Bench-Tested Circuits for Surveillance and Countersurveillance Technicians*, I call for the use of a sensitive-gate SCR (silicon, controlled rectifier). At times these sensitive-gate SCRs are hard to come by, so I thought I would help you out a little by throwing in this handy little circuit. It uses very common, easy-to-obtain components. You may find that this circuit is much more reliable and glitch-free than an SCR; however, it will take up much more space (precious circuit board real estate).

Please remember the following when using this SCR replacement circuit: when the circuit that this device is connected to is powered up, you will probably need to momentarily push the reset switch due to the output glitch on power-up.



PARTS LIST:

Q1 – 2N3904 OR 2N2222 general-purpose NPN silicon transistor
K1 – 9- TO 12-VOLT, 500 to 1,000-ohm DPST or DPDT relay
Two 1K resistors
One optional LED
Normally closed push-button switch
D1 – 1N914 silicon diode for "spike prevention"

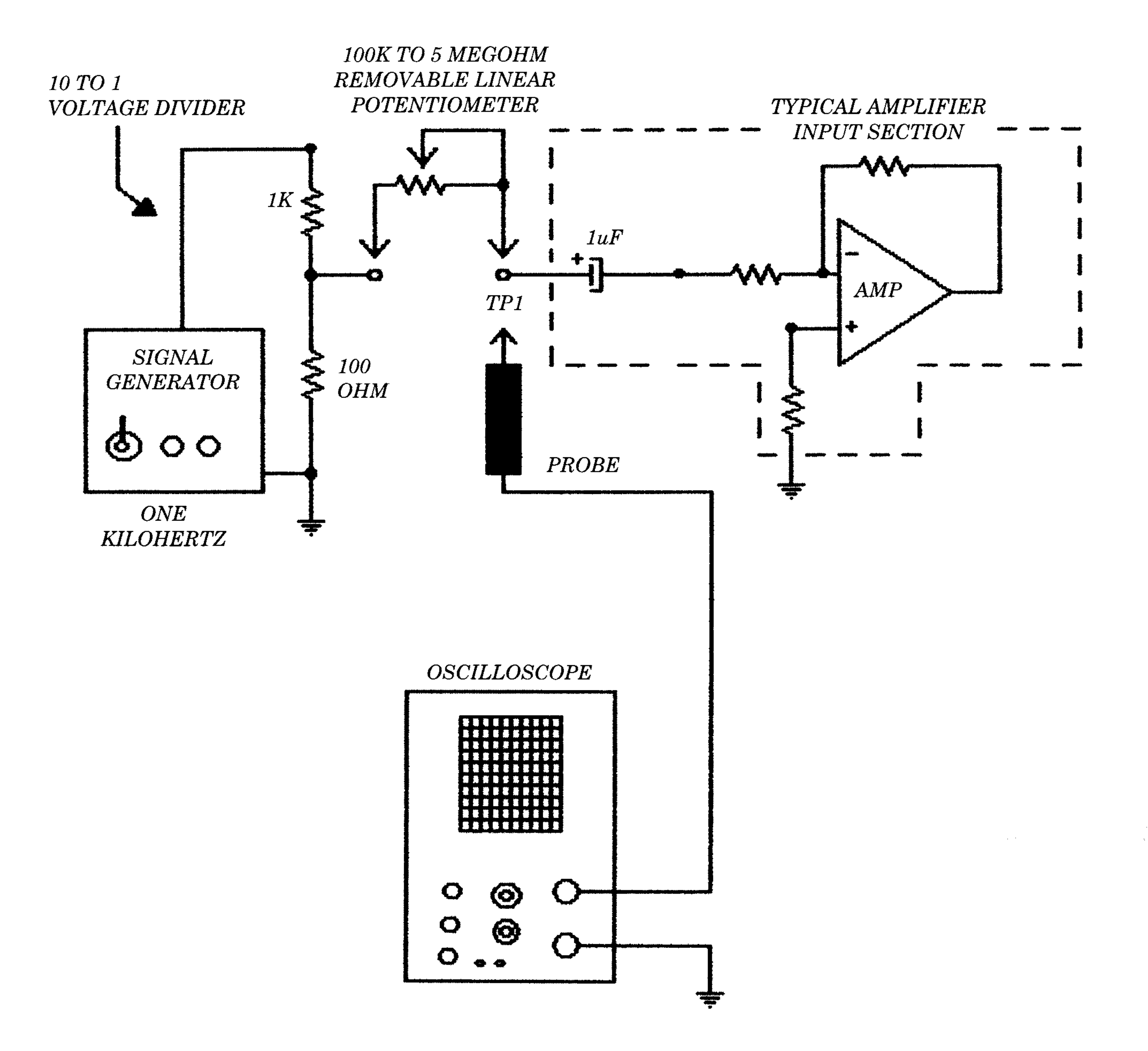
APPLICATIONS NOTE: When a positive pulse arrives at the base of Q1, the transistor turns on, latching the two normally open relay contacts to the closed position. Contacts (A) keep the base of Q1 at a positive potential, while contacts (B) operate the external circuit to be controlled.

HOW TO TURN A DPST RELAY INTO AN SCR (YOU WON'T NEED A SENSITIVE-GATE SCR WITH THIS CIRCUIT!)

HOW TO MEASURE INPUT IMPEDANCE

Here is a handy technique for measuring the input impedance to various "experimental" audio amplifiers and preamps. This diagnostic technique gives you the real input impedance—not the theoretical input impedance. In actual practice, other authors, including myself, have been off by as much as 50 percent (actual vs. theoretical) when estimating impedance. This circuit should eliminate speculation.

Let's take a closer look. The voltage divider prevents any loading of the signal generator when connected to the input of a preamp or amp as long as the impedance of the preamp or amp is much higher than 100 ohms. In almost all instances the input impedance to most amplifiers and preamps will be much greater than 100 ohms. When the signal generator is adjusted for a one volt peak to peak, 1kHz, reading across the 1k resistor, there will be approximately 100 millivolts peak to peak across the 100-ohm resistor. This 100 millivolts will be highly readable with most scopes, yet it will not overdrive and cause distortion to small covert—oops, I mean "experimental"—amps and preamps.



APPLICATION NOTES: Adjust signal generator to 1kHz and adjust output level so that one volt is measured across the 1K resistor. Adjust the potentiometer for maximum reading at TP1 (Test Point 1) and note the reading. Then, adjust the potentiometer for one half reading at TP1. Now, remove the potentiometer and measure the resistance. The resistance measured across the potentiometer is the ballpark input impedance of the circuit you are measuring. All readings are peak to peak. Readings taken from TP1 are relative. You will need a large resistance value for the potentiometer when you are measuring high impedance circuits.

HOW TO MEASURE INPUT IMPEDANCE

TWO TONE GENERATOR FOR WIRE TRACING

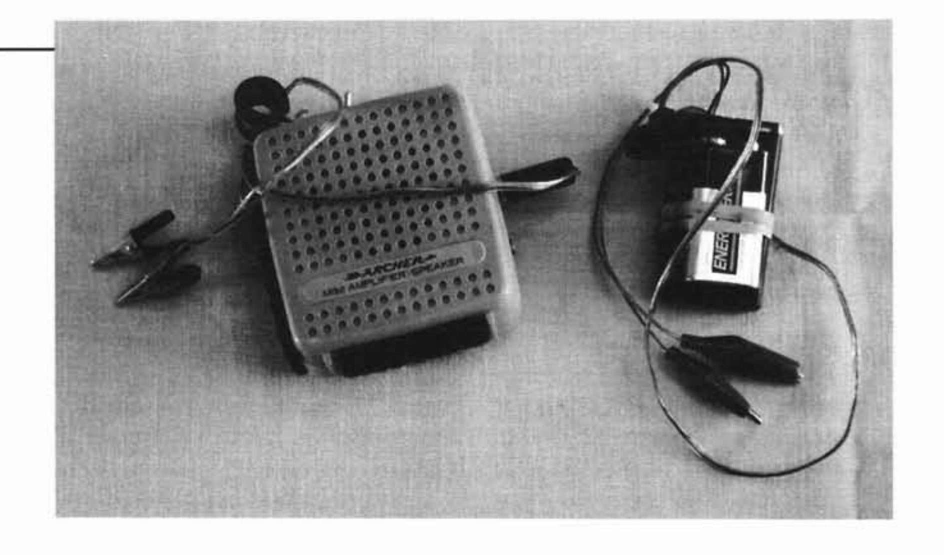
This circuit is great for wire tracing when used with the inductive probe circuit as outlined elsewhere in this book. The output sounds similar to a British siren. Since the tone is so distinctive, it's hard to mistake when tracing wire pairs.

The output is a square wave that is rich in harmonics. The author was able to receive the tones loud and clear on a portable AM radio (tuned to a blank channel) from more than 5 inches away. It is possible to trace wires through walls and ceilings by using an AM radio as just described.

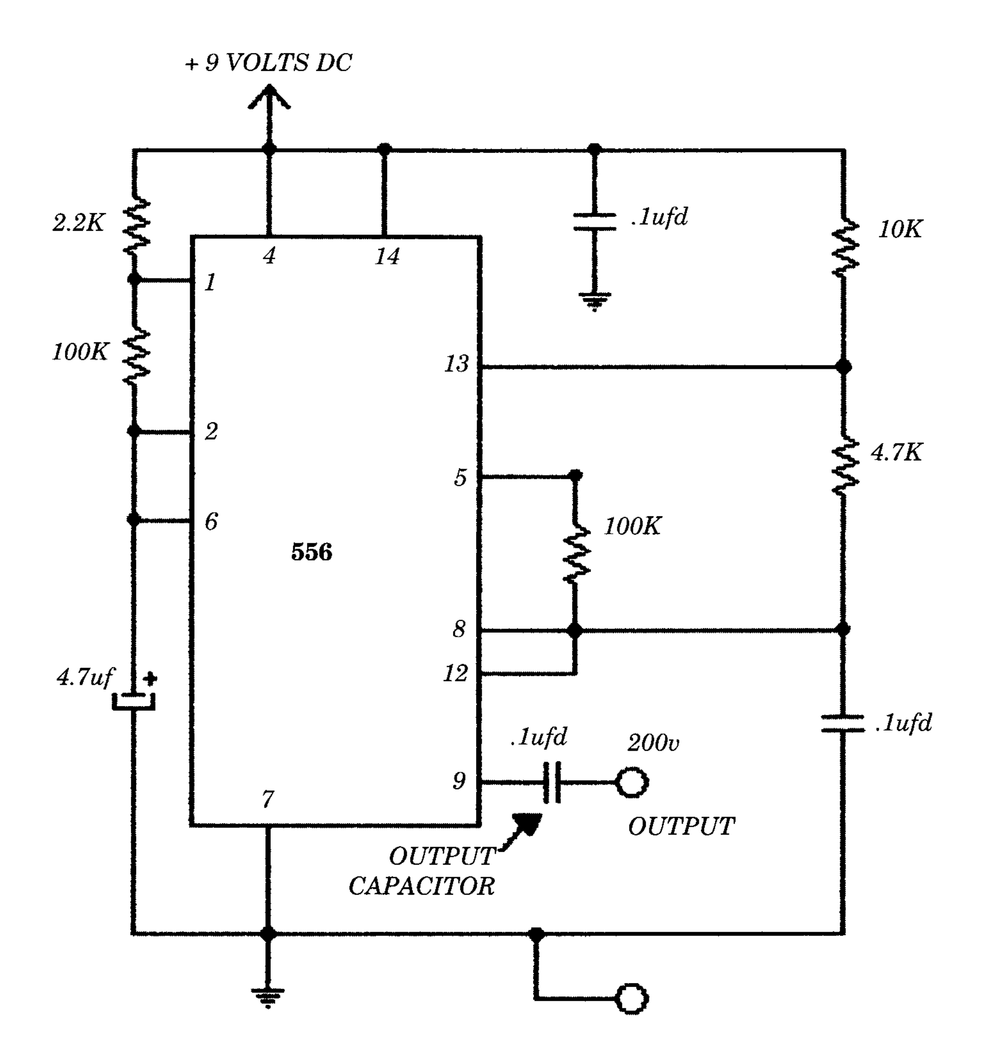
When I perform a countermeasures sweep and need to trace some wire pairs, all I do is bring along my old Radio Shack amplifier and the "Two Tone Generator." I installed a .01uF capacitor at the input of the amp to block DC and to pass audio. I also installed a patch cord with alligator clips at one end and a miniature plug for quick connection to the amp. I put the "Two Tone Generator" in a small plastic box with a 9-volt battery strapped to the outside with a large rubber band. I also connected a 2-foot patch cord with color-coded alligator clips to the "Two Tone Generator." Most of the time all you need to do is just touch one probe tip (alligator clip) to one of the wire pairs under test.

A possible scenario for the "other side": an operative could hop the fence in a suburban backyard and place this device on the phone line at the surge protector box. Then the operative goes to the big area interface box on the street corner usually located within a half-mile radius of the home and starts probing for the signal on the neat rows (and rows) of connectors. Once he finds the "target" wire pair, the fun begins! Then he goes back to pick up his "Two Tone Generator."

Please be nice to the dog . . .



Here is the "Two Tone Generator for Wire Tracing" packaged in a small plastic Tic-Tac case spray-painted black. The author installed a .01uF capacitor in-line with the patch cord to the amplifier in order to block DC voltage from the phone line. Without the capacitor, the amplifier would "load" the phone line and trip the central office circuits.

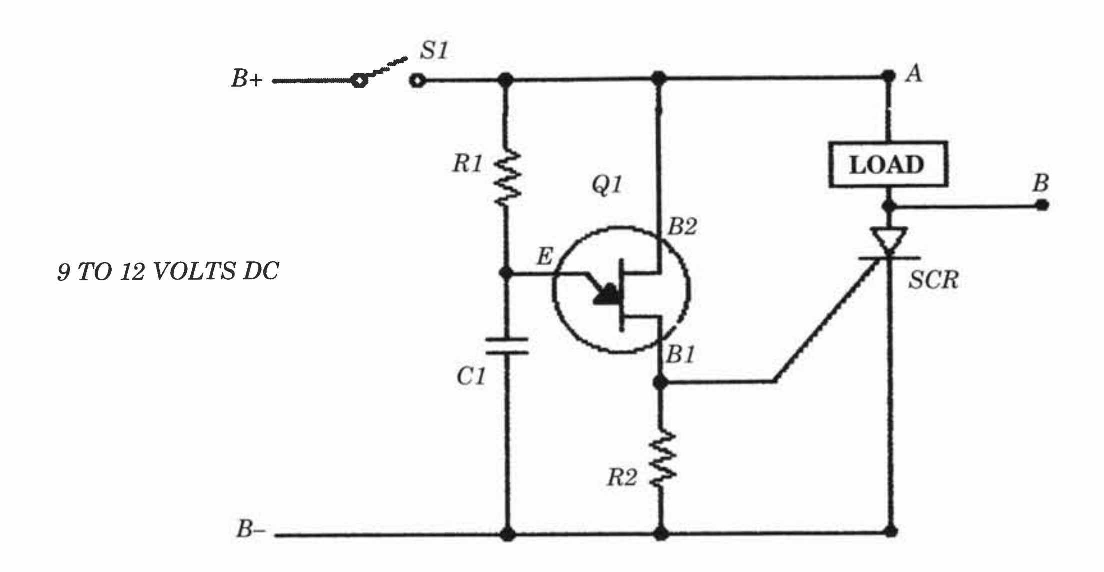


CONSTRUCTION NOTES: A patch cord with alligator clips should be attached to output and ground. A small plastic Tic-Tac case, spray-painted black, would make an ideal housing for this project.

OPERATIONAL NOTES: This circuit will emit a pleasant "British siren" type sound. This circuit is very handy for tracing and identifying unknown wire pairs. Do not connect to high-voltage (115 volts AC and above) circuits unless the breaker is shut off. Connection to active phone pairs and other DC circuits is OK due to output capacitor, which will block DC voltage.

TWO TONE GENERATOR FOR WIRE TRACING

GLITCH-FREE, ON-AFTER-DELAY TIMER



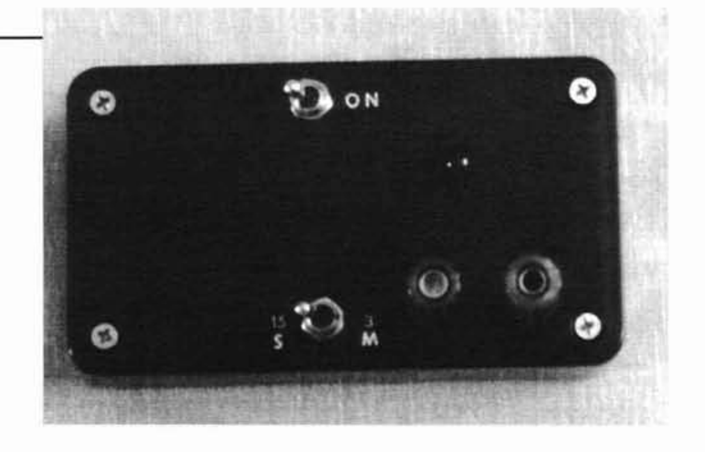
PARTS LIST:

Q1 – 2N2646 or equivalent UJT (unijunction transistor)
C1 – 10ufd to 1,000ufd electrolytic capacitor (sets time delay)
R1– 100K to 1Meg 1/4-watt resistor (sets time delay)
R2 – 100 ohm 1/4-watt resistor
SCR – sensitive-gate SCR (don't use the typical 100- to 300-volt types)
S1 – SPST switch
LOAD – could be a 500- to 1,000-ohm 6- to 12-volt relay or a small 6- to 12-volt DC flashlight bulb. Even a portable DC radio could be used as a load.

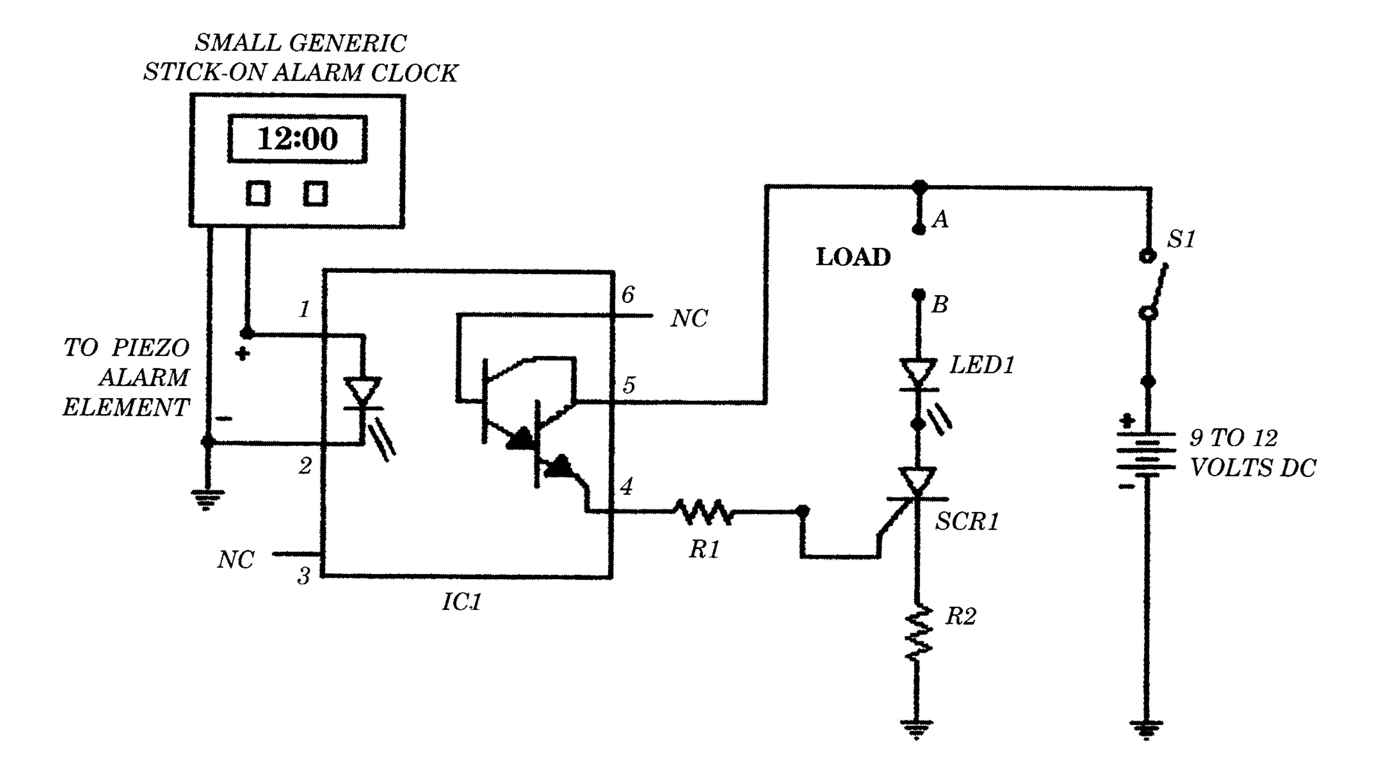
NOTE: (Worst-case scenario.) Points A and B can be tested with an analog meter, test light, or oscilloscope in order to determine the magnitude of an output glitch and see if it will be a significant factor.

IMPORTANT TIMING NOTE: The time constant R1xC1 does not seem to apply in actual test cases. You will have to do your own calibration for time delay.

Here is the "glitch-free on-after-delay timer." I modified this versatile timer with a time-selection switch (15 seconds and 3 minutes). An LED was connected in series with the SCR for output status indication.



A TIMER JAMES BOND WOULD BE PROUD OF



NOTE: The load could be a 6- to 9-volt Radio Shack-type relay with a 500- to 1,000-ohm coil in series with a switch. Connect between A and B. You will need to remove R2 if you use the relay. Remember Ohm's Law—relay will not pull in with R2. Some applications with low-voltage and low current will not require a relay at points A and B. Be sure to follow sequence in order to avoid the output glitch on power up.

PARTS LIST:

IC1 – photo darlington optocoupler 4N32, 4N33, or equivalent
R1 – 220 ohm 1/4-watt resistor
R2 – 330 ohm 1/4-watt resistor
LED1 – light-emitting diode
SCR1 – silicon-controlled rectifier (sensitive-gate type)
S1 – SPST switch (mini)

IMPORTANT CONSTRUCTION NOTE: Pin 1 goes to + on piezo element, pin 2 goes to – on piezo element. Carefully pull alarm housing apart and look for a metal disc. You may need to reverse pin 1 and 2. You may also need to experiment with grounding or not grounding pin 2 on IC1.

SEQUENCE:

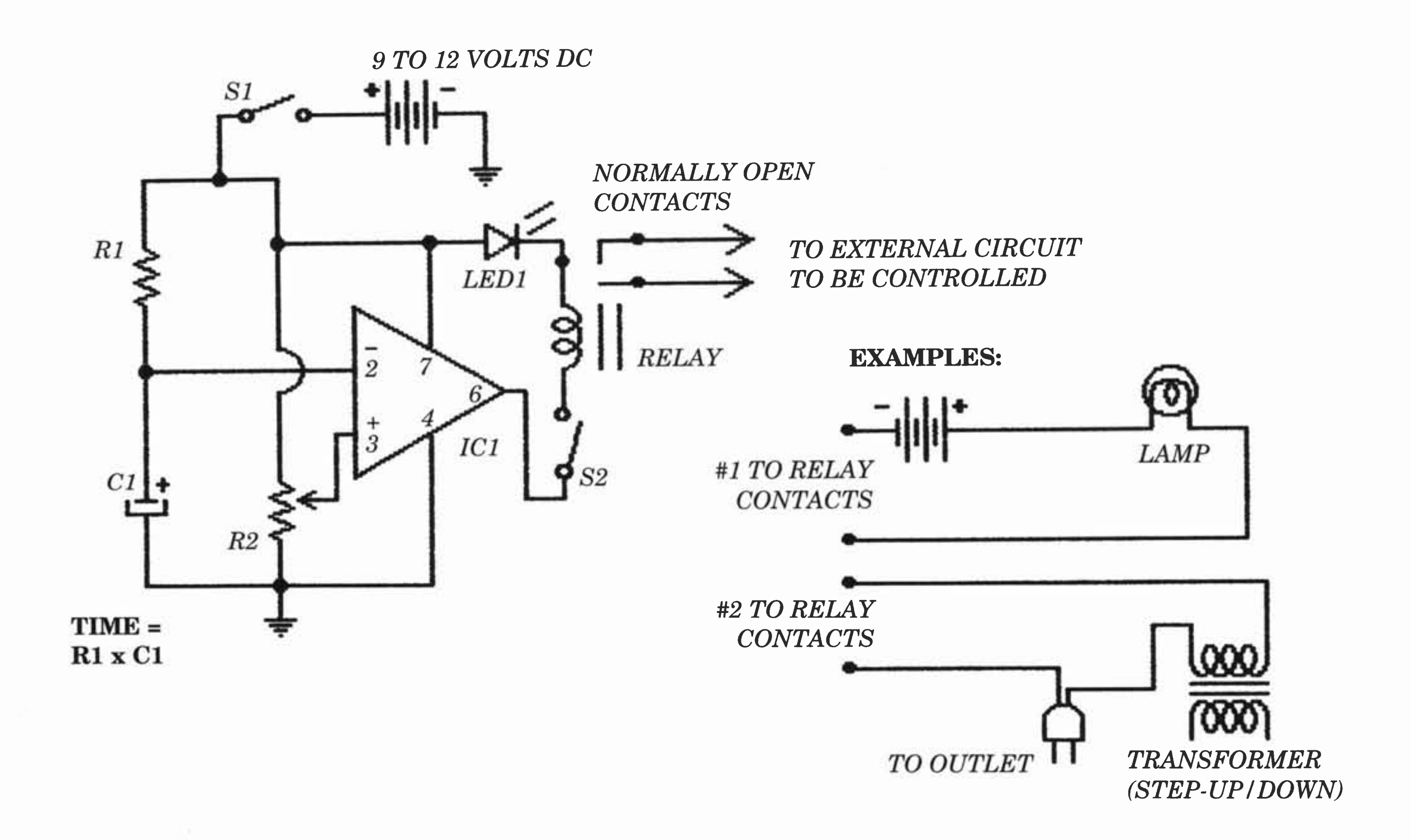
1 – SET ALARM

2 – CLOSE S1

3 – CONNECT LOAD

ONE COULD PUT SWITCH IN SERIES W/ LOAD.

TIMER—ON AFTER DELAY



PARTS LIST:

IC1 – 741 op-amp (very common analog IC)
LED1 – red LED (light-emitting diode, optional)
RELAY – 1,000-ohm 6- to 9-volt relay
C1 – 10ufd to 6800ufd electrolytic capacitor (sets time delay)
R1 – 100K ohms to 1 megohm 1/4 -watt resistor (sets time delay)
R2 – 100K ohms (PC board mount trimpot) sets the reference voltage
S1 – SPST switch
S2 – SPST switch for safety (prevents false triggering)

IMPORTANT: S2 is needed due to the fact that there is an output glitch during the initial power-up when S1 is closed. Relay contacts should be rated to handle the load.

INITIAL ADJUSTMENT: During initial adjustment, use small values for R1 and C1 (100K and 5uF). R2 should be set to its middle point and adjusted slightly from there.

SEQUENCE:

1) CLOSE S1

2) CLOSE S2

APPENDIX: SUPPLIERS

ALL ELECTRONICS CORP.
905 S. Vermont Ave.
Los Angeles, CA 90006

AMERICAN SCIENCE & SURPLUS
3605 Howard Street
Skokie, IL 60076

C and H SALES COMPANY
P.O. Box 5356
Pasadena, CA 91117

DC ELECTRONICS
P.O. Box 3203
Scottsdale, AZ 85257
Optical Devices (Lenses):

EDMUND SCIENTIFIC
C912 Edscorp Bldg.
Barrington, NJ 08007

ELECTRONIC GOLDMINE
P.O. Box 5408
Scottsdale, AZ 85261

GATEWAY ELECTRONICS
2525 Federal Blvd.
Denver, CO 80211

FISTELL'S MICRO ELECTRONICS
7023 E. Colfax
Denver, CO 80220

HERBACH AND RADEMAN
P.O. Box 122
Bristol, PA 19007

MARLIN P. JONES & ASSOCIATES INC.
P.O. Box 12685
Lake Park, FL 33403

MOUSER ELECTRONICS
2401 HWY 287 N.
Mansfield, TX 76063

R&D ELECTRONICS
1224 Prospect
Cleveland, OH 44115

RADIO SHACK NEAREST YOU!
Check your hometown Yellow Pages
under Electronics Parts.

SURPLUS CENTER
P.O. Box 82209
Lincoln, NE 68501